

Efficient Vehicle-level Coordination in Functional Safety Process for a Whole Vehicle

Takashi OHTA* Hiroki SAGAMI*

ABSTRACT

On-board logical electrical and/or electronic systems are required to comply with functional safety standard ISO 26262. Functional safety activities involve implementing a standard-compliant process as a measure to help prevent any physical injury or damage to human health that may be caused by system malfunctions. In order to efficiently comply with ISO 26262 in automotive development relating multiple systems intricately, the personnel working on each system need to rationally coordinate and implement the functional safety activities for a whole vehicle. Honda has therefore added to the functional safety process its own process of coordinating functional safety requirements. The process involves investigating how the systems of the whole vehicle relate at the vehicle level, formulating methods to allow necessary and sufficient boundaries of functional safety activities to be set, conducting impact analyses cooperatively by using the system interfaces as guides, and coordinating the functional safety requirements. This eliminates the overlap in impact analysis scope, improving accuracy for system internal impact analyses. Further, adding the proprietary process to link systems has resulted in exhaustive implementation of high-precision impact analyses at the vehicle level, in turn forming a vehicle-level functional safety process for the whole vehicle capable of appropriately deploying functional safety requirements.

1. Introduction

With the number and complexity of electronic control systems on the rise in modern vehicles, functional safety standard ISO 26262 (Fig. 1) was formulated, officially going into effect in November 2011⁽¹⁾. Generally, on-board electrical and/or electronic (E/E) systems use equipment such as switches, sensors, and communication devices to digitize and input driver operation status and vehicle status, and then use the input information to control one or more systems and perform functions. If a system malfunctions, the driver or system is unable to control the mechanisms as intended, resulting in hazards (Fig. 2).

With ISO 26262, in addition to intrinsic safety, development is required to determine the causes for any failure in an E/E system causing hazards resulting in physical injury or damage to human health, and to apply measures to reduce hazard risks to acceptable levels. These activities are required for each item, consisting of a system or array of systems that implement a function at the vehicle level. Before ISO 26262 went into effect, systems to be developed were mainly managed by electronic control units (ECU) and specific functional units. Thus, hazard analysis

and risk assessment (H&R) for items has been performed for each system, with functional safety requirements assigned to each system before performing the activities in ISO 26262 from Part 4, “Product development at the system level,” to the end (Fig. 1). As ISO 26262 (Fig. 1) is a waterfall-type V-model development process, any

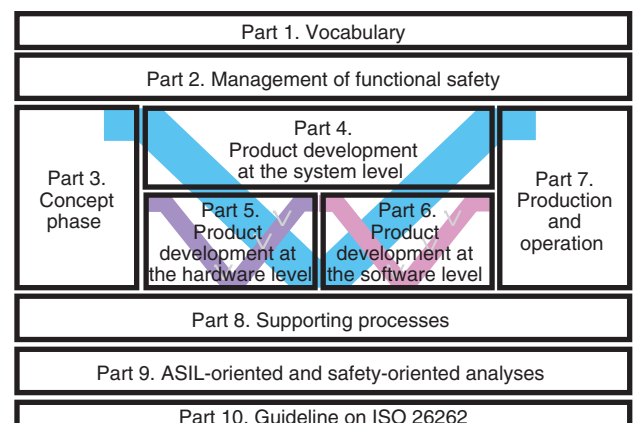


Fig. 1 Overview of ISO 26262

* Automobile R&D Center

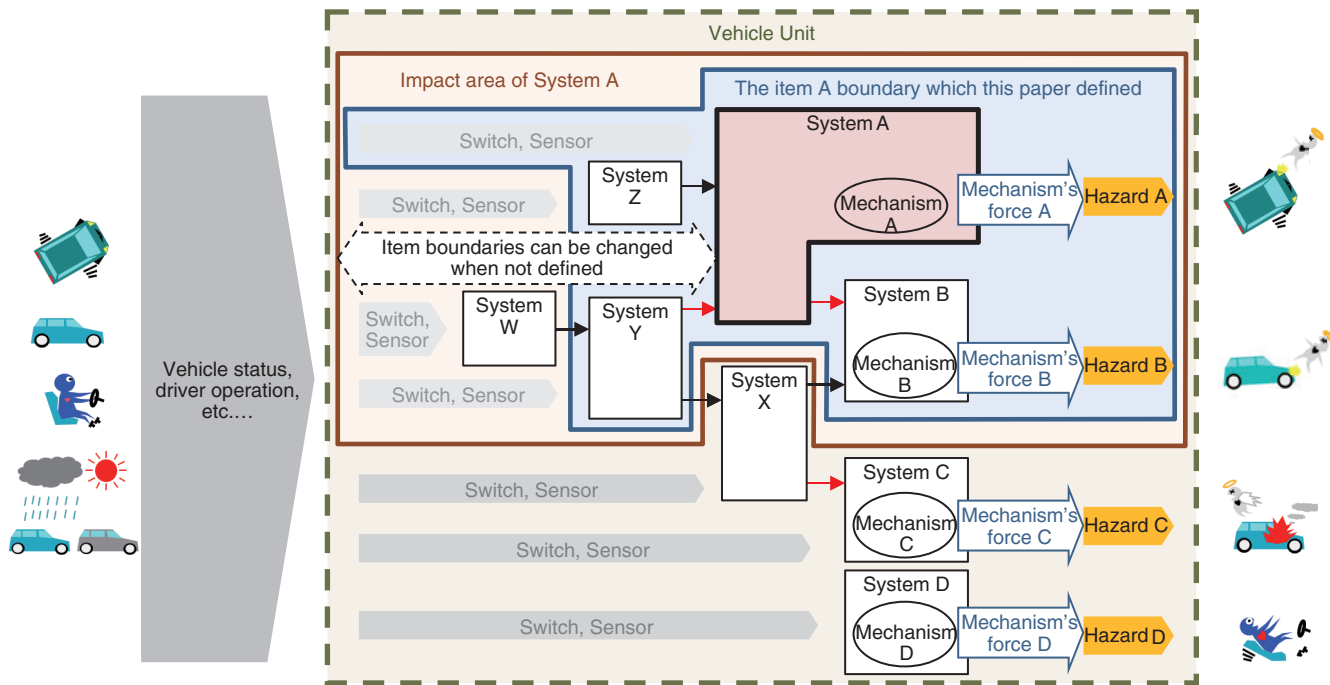


Fig. 2 Relationship among systems, item boundaries, and vehicle level

omissions or oversights in design and analysis performed in the upstream part of the process will require many man-hours to rework, in turn increasing work time in the downstream parts of the process. Thus, how precisely the impact analysis can be completed in the upstream part of the process with well-organized item boundaries is the key to efficiently achieving functional safety at the vehicle level. However, while the functional safety process is defined in ISO 26262 for individual items, it is not clearly defined for coordinated development of multiple items at the vehicle level. Honda has therefore developed a functional safety process for a whole vehicle. The process allows functional safety requirements to be deployed appropriately for the whole vehicle in order to resolve the aforementioned issues in ISO 26262 Part 3, “Concept phase,” corresponding to the upstream part of the functional safety process.

2. Development Goals

In ISO 26262-compliant development, functional safety activities are required for the items. However, given that different system personnel may define item boundaries differently, rework due to omissions and oversights as well as waste due to duplicate work will occur at the vehicle level unless item boundaries are set according to fixed rules. The completeness and accuracy of impact analysis in the upstream part of the process will impact efficiency downstream. If items are not properly coordinated upstream in the process, extra time will be required to verify that the analysis scope is complete even if complementary functional

safety activities are performed in the other systems. Further, having personnel for the individual systems set the scope for analysis any larger than their own systems is inefficient as it will result in personnel for multiple systems analyzing duplicated scope. Moreover, given how carry-over has been integrated into the development scheme to help reduce man-hours, the process presented in this exercise must also allow reuse of development resources.

In light of the above points, in order to perform highly precise functional safety activities efficiently at the vehicle level, the goals for the functional safety process for the whole vehicle presented in this exercise were determined to be as follows:

- (1) Clearly specifies the paths of transmission (interface) between systems for hazard impacts and functional safety requirements.
- (2) Creates a scheme for deciding item boundaries so that unnecessary overlap in impact analysis scope is minimized.
- (3) Creates a functional safety process for a whole vehicle so that impact analyses for hazards can be coordinated between systems, and that functional safety requirements can be assigned and coordinated.

3. Functional Safety Process for the Whole Vehicle

A functional safety process for the whole vehicle was developed by adding the processes linking the various systems to the existing functional safety process based upon

the schemes for interface classification and hazard impact transmission described below.

3.1. Interfaces Clarified

3.1.1. Interface classifications

This process is characterized by using interfaces as guides for activity. These interfaces are classified into three categories: mechanism's force, operation requests, and information. Mechanism's force interfaces communicate physical effects, and operation request interfaces manipulate the mechanism's force of other systems. Meanwhile, interfaces are classified as information interfaces when it is unclear whether it has any direct impact upon a hazard.

3.1.2. Scheme for hazard impact transmission

Examples of how hazard impacts are transmitted are given in Figs. 3(a)-(d). In the figures, systems are represented as squares, mechanisms as ellipses, information interfaces as black arrows, operation request interfaces as red arrows, mechanism's force interfaces as blue-gray arrows, and hazards as orange arrows. For example, in Fig. 3(a), a hazard occurs when System E erroneously controls the mechanism due to an internal malfunction in System E, with the mechanism generating an abnormal force. Meanwhile, in Fig. 3(b), a hazard occurs despite System F not having a mechanism when System F outputs an operation request to System G, impacting System G's mechanism. Next, in Fig. 3(c), the impact of a hazard caused by the mechanism of System J is transmitted all the way to the switches, sensors and other vehicle-level input devices via information, System I and System H. Possible means of reducing the impact of such a hazard include implementing a safety mechanism in the system located between the hazard and vehicle-level input devices [Fig. 3(d)].

The standard architecture shown in Fig. 5, with the interfaces clearly specified between the systems, was created based on the above interface classifications and schemes for hazard impact transmission. Using this standard architecture with the interfaces as guides, a process was developed in which system personnel perform their impact analyses cooperatively and coordinate functional safety requirements. This helps system personnel to easily identify what risks exist in their systems, as well as the risk source and scale, facilitating appropriate assignment of functional safety requirements.

3.2. Overlap Reduced in Impact Analysis Scopes

3.2.1. Item boundary conditions

As illustrated in Section 3.1.2., systems are thought to output mechanism's force and operation requests that directly result in hazards, or to indirectly cause hazards through information. As safety measures can be implemented across all paths resulting in the hazards if functional safety requirements are properly assigned between adjacent systems, item boundary conditions have

been set as follows.

When interfaces are input, the systems and their mechanisms linked via those interfaces are included in the item scope. Meanwhile, when interfaces are output, the systems and their mechanisms linked via those interfaces,

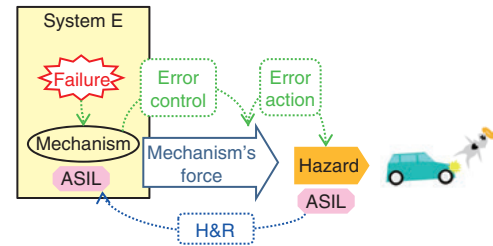


Fig. 3(a) Hazard occurrence

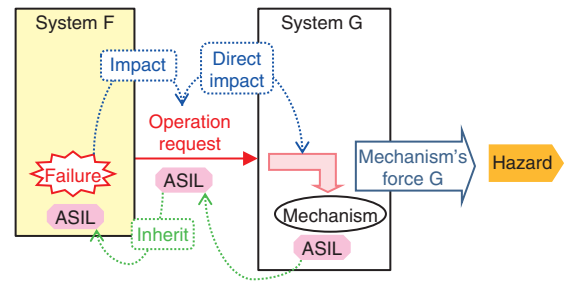


Fig. 3(b) Hazard due to operation request

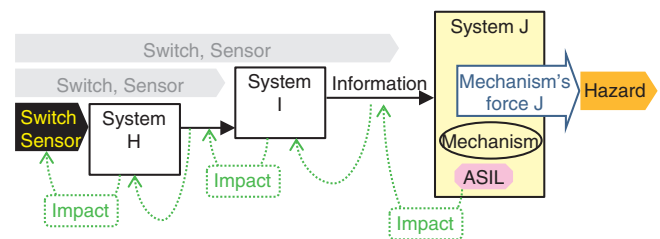


Fig. 3(c) Transmission path of hazard impact

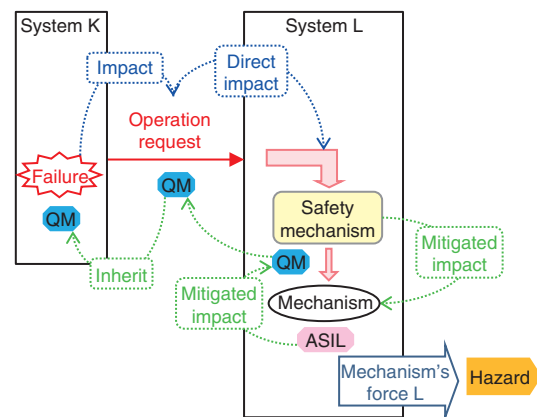


Fig. 3(d) Mitigation of hazard impact by safety mechanism

mechanism's force, and related hazards are included in the item scope.

3.2.2. Preconditions

Preconditions for the process are as follows. The scale of hazard impact as transmitted via each interface is expressed in terms of ASIL. In addition, personnel are posted for each system, with the personnel implementing safety measures for the functional safety requirements assigned to their systems, working as described in ISO 26262 from Part 4, "Product development at the system level," to the end (Fig. 1).

The standard architectures were created based on the above item boundary conditions and preconditions, with item boundaries organized for a whole vehicle. With unneeded overlap in impact analysis scope reduced by developing a process for system personnel to perform their impact analyses cooperatively using these standard architectures, system personnel can concentrate on analyzing the impacts within their own systems.

3.3. Functional Safety Process for the Whole Vehicle

System personnel and Process Manager work together to implement Processes (1)–(6) as given below. System personnel perform Processes (2)–(4) and (6) for the item of each system as the scope for their functional safety activities. Meanwhile, the Process Manager manages the progress for each system and implements the functional safety activities for the whole vehicle (Fig. 4).

Process 1: Process Manager creates and distributes basic architectures for each item in the vehicle under development

Process 2: System personnel create preliminary architectures

Process 3: System personnel perform hazard impact analyses

Process 4: Functional safety requirements coordinated between system personnel

Process 5: The Process Manager updates standard architectures

Process 6: System personnel perform functional safety activities in ISO 26262 from Part 4, "Product development at the system level," to the end (Fig. 1)

Processes (1)–(6) are described in detail below.

3.3.1. Process Manager creates and distributes basic architectures for each item in vehicle under development

The Process Manager investigates on-board vehicle systems and their related systems and applies the item boundary conditions given in Section 3.2.1. to create the standard architecture (Fig. 5). At the onset of vehicle development, the Process Manager checks the on-board systems for the vehicle under development, creates basic architectures from the standard architecture, restricting them to the necessary systems, and distributes the basic

architectures to personnel for each system (Fig. 6).

3.3.2. System PIC creates preliminary architecture

Based on the basic architecture, a person in charge of the system (system PIC) coordinates with the personnel from related systems to specify which interfaces will be used (or not used) for the vehicle under development and creates a preliminary architecture for his/her own system (Fig. 7). When creating the preliminary architecture, the system PIC coordinates with the personnel from related systems if the interfaces and related systems are insufficient, and requests the Process Manager to change the preliminary architecture.

The Process Manager will then update the preliminary architecture for the system to be changed.

3.3.3. System PIC performs hazard impact analysis

For systems outputting their mechanism's force, the system PIC performs H&R for his/her own system and evaluates the ASIL(s) for the hazard(s) of the mechanism's force. For the system with an operation request that acts upon the mechanism's force with the ASIL being input, the system PIC will assign the ASIL to the operation request input to his/her own system and inform the PIC of the system outputting the operation request. Next, the PIC of the system outputting the operation request confirms the reported ASIL and assigns the reported ASIL to the operation request being output (Fig. 8).

The system PIC then produces a concept design for his/her own system with the assumed allocation of safety mechanism elements and performs an impact analysis within the system. The PIC assigns ASILs to the interfaces implemented in the system and informs personnel for related systems (Fig. 9). Finally, the PIC will check the ASILs assigned to the interfaces in his/her own system to confirm the validity of the safety mechanisms as assumed

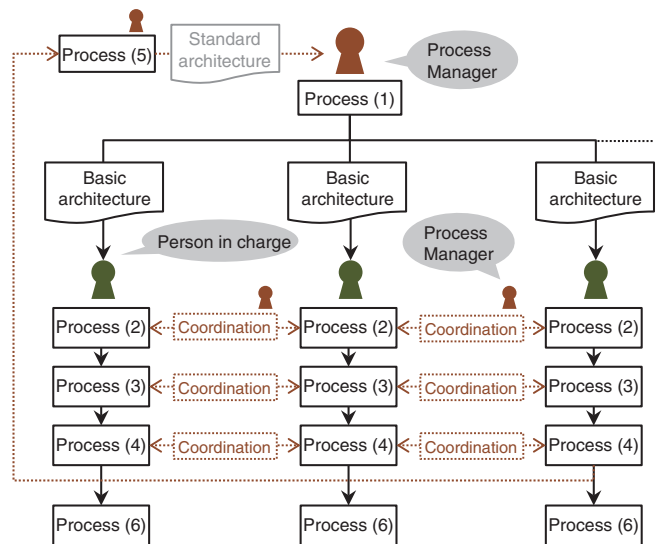


Fig. 4 Functional safety processes at vehicle level

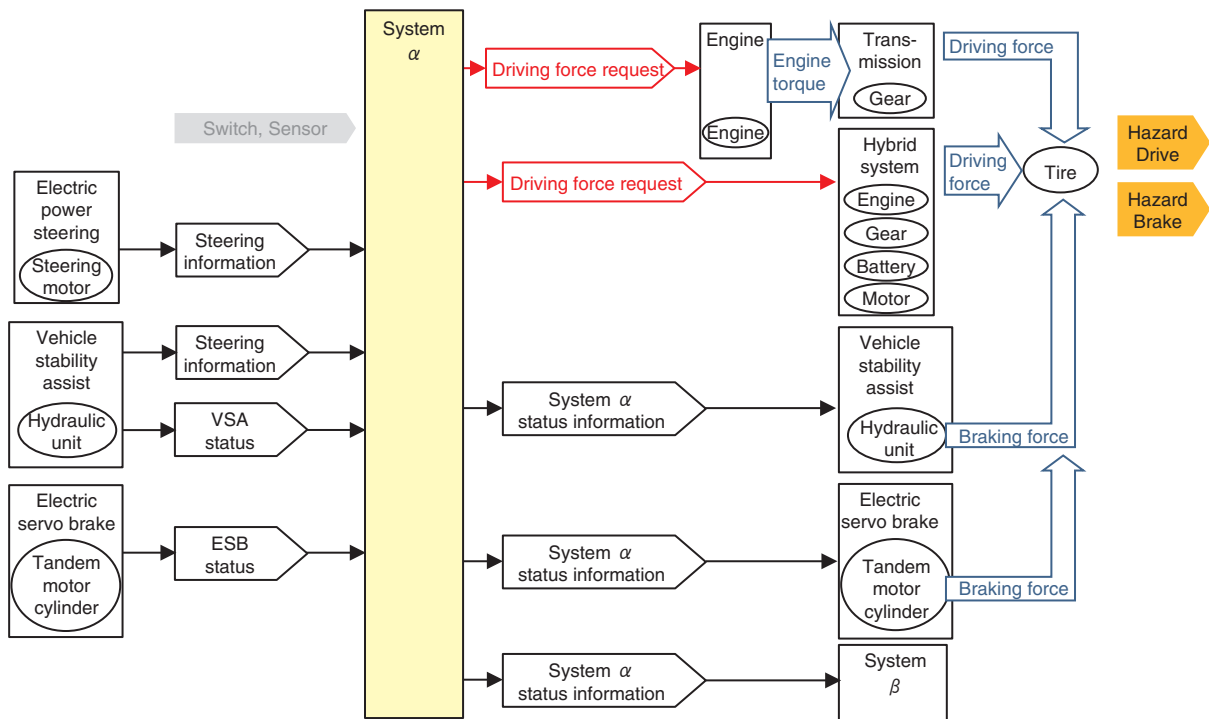


Fig. 5 Standard architecture

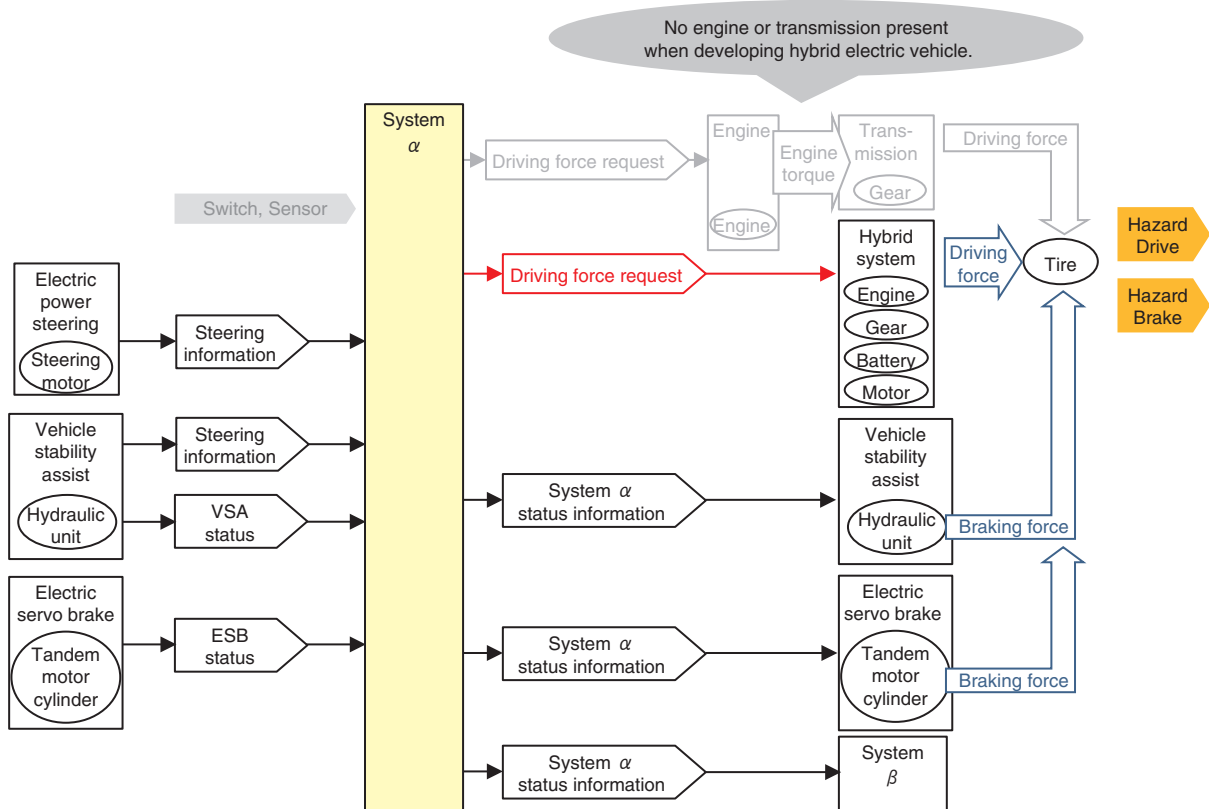


Fig. 6 Basic architecture

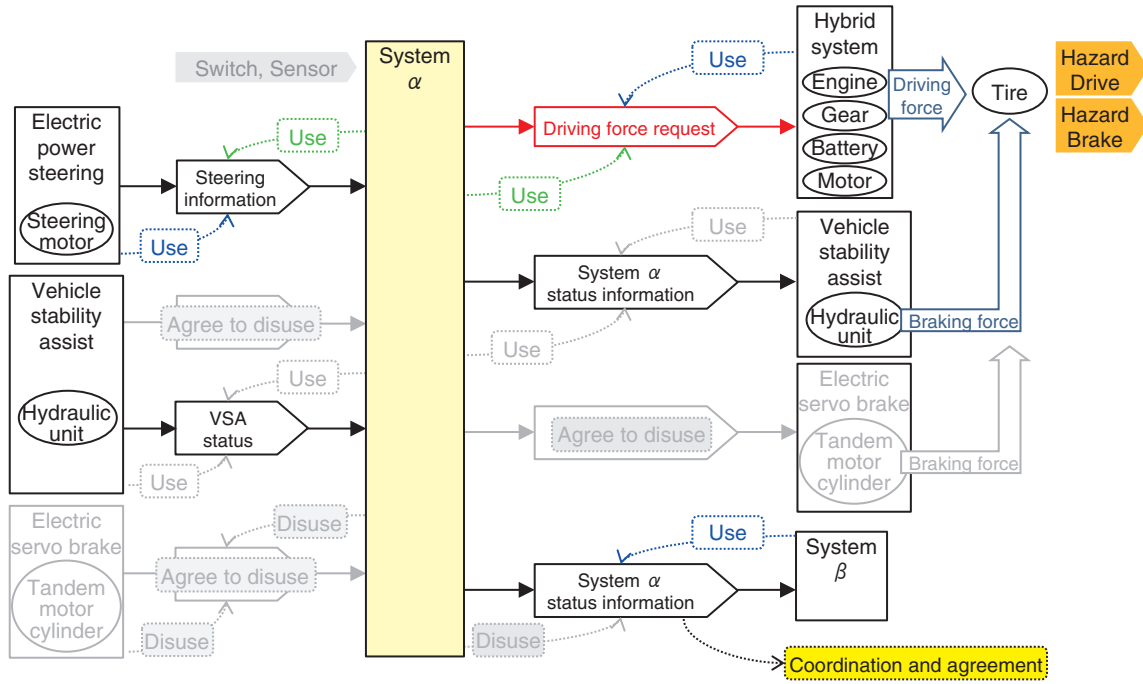


Fig. 7 Process of creating preliminary architecture

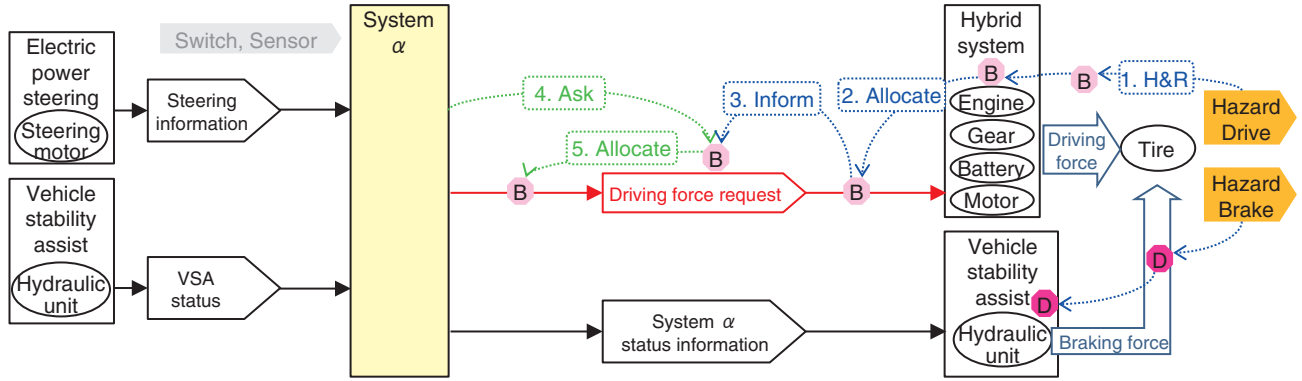


Fig. 8 Hazard analysis and risk assessment of mechanism's force and impact analysis of operation request

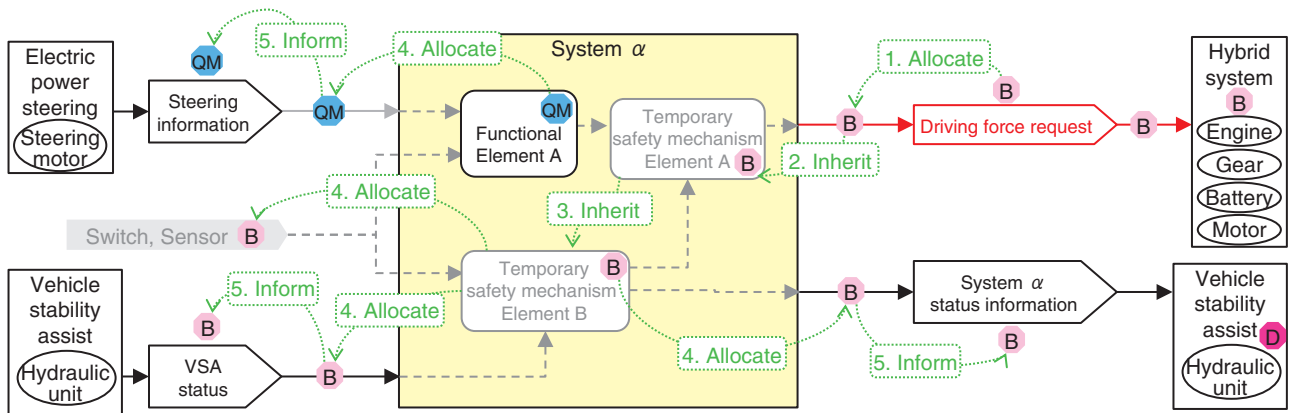


Fig. 9 Concept design assuming allocation of safety mechanisms, and impact analysis between systems

in the concept design. If, for example, a higher ASIL than expected has been assigned, concept design and impact analysis is redone (Fig. 10).

3.3.4. Functional safety requirements coordinated between system personnel

The system PIC assigns the functional safety requirements to the system interfaces with ASILs assigned. When safety mechanisms for those interfaces are to be

implemented by related systems, the PIC assigns and coordinates the functional safety requirements and agrees upon their details with personnel for the related systems (Fig. 11). When confirming and coordinating functional safety requirements assigned from related systems, the system PIC is to agree upon functional safety requirements with personnel from the related systems when such requirements are assigned to the system interfaces from the related systems (Fig. 12).

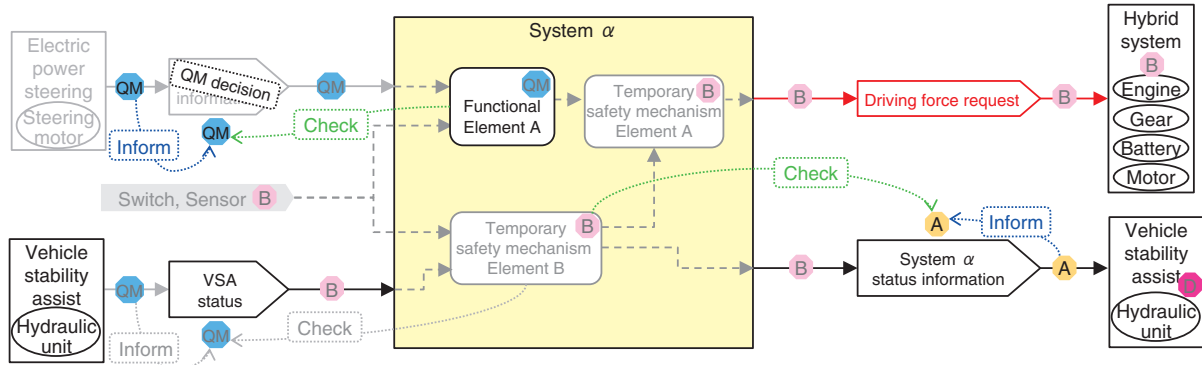


Fig. 10 Check for allocated ASILs

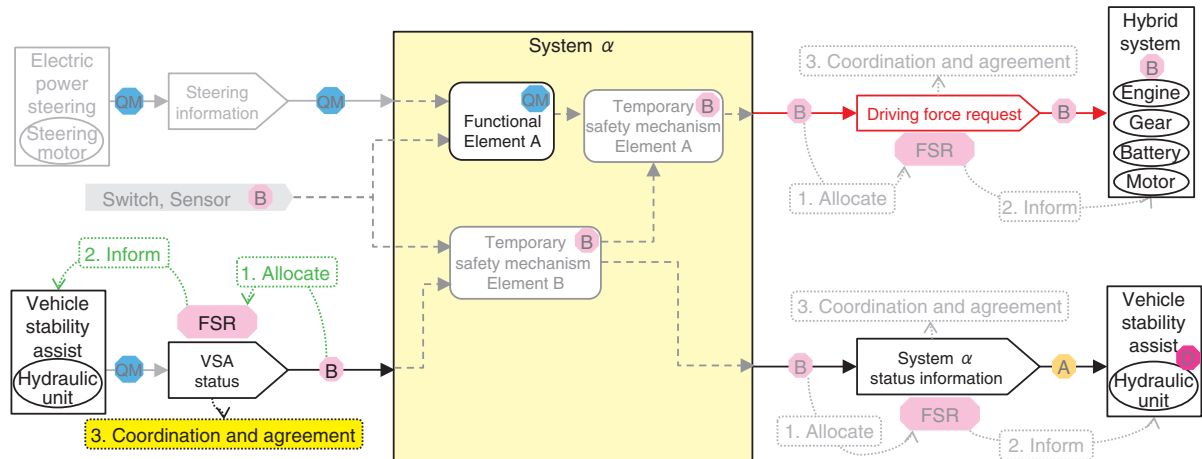


Fig. 11 Coordination and agreement of functional safety requirements assigned to other systems

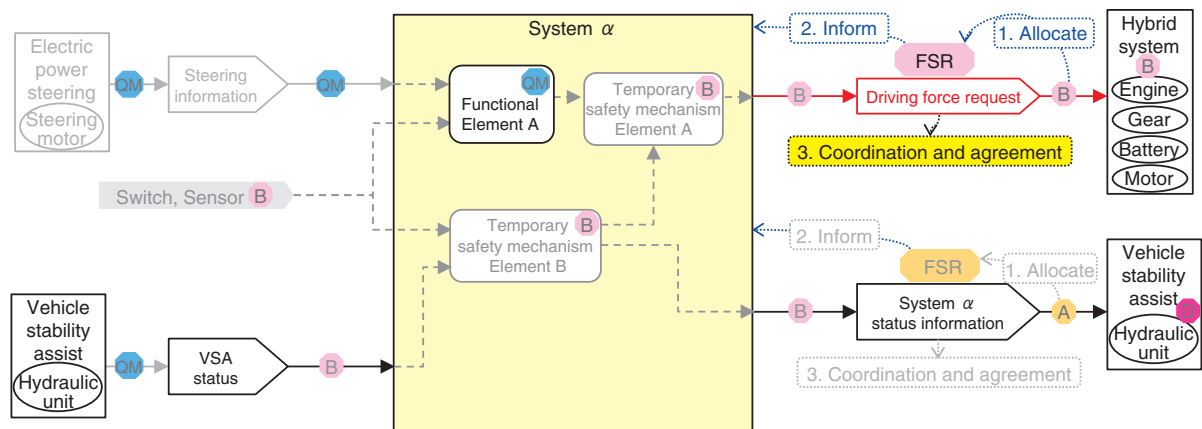


Fig. 12 Coordination and agreement of functional safety requirements assigned from other systems

3.3.5. Process Manager updates standard architectures

If new interfaces are added to the completed architectures, the Process Manager is to add the additional interfaces to the standard architectures.

The updated standard architectures will then be used as a development resource for subsequent vehicles.

3.3.6. System personnel perform functional safety activities in ISO 26262 from Part 4, “Product development at the system level,” to the end

Functional safety requirements assigned to a system in the activities described in Section 3.3.1.-3.3.5. are added to the requirements originally assigned within the system before functional safety activities from Part 4 to the end are implemented⁽²⁾.

Organizing item boundaries for the whole vehicle as given above and developing a functional safety process for the whole vehicle to be implemented through coordination of system personnel using standard architectures with inter-system interfaces clearly specified has made it easier to spot omissions and oversights in the assignment of functional safety requirements in vehicle-level functional safety activities. Further, highly polished standard architectures created after the coordination of functional safety requirements can be incorporated in development of subsequent vehicles, which has made the development with carry-over easier. Thus, an efficient functional safety process has been developed for the whole vehicle.

4. Conclusion

The development of this process has produced the following outcomes:

- (1) System interfaces have been classified into the mechanism’s force, operation requests, and information, and how the systems interrelate have been clearly specified. This helps system personnel to easily see what risks exist in their systems, as well as the source and scale, facilitating appropriate assignment of functional safety requirements.
- (2) Item boundary conditions are set with the systems and their mechanisms linked via interfaces, with the mechanism’s force and related hazards included in the item scope. This has reduced unneeded overlap in impact analysis scope, allowing system personnel to concentrate on analyzing the impacts within their own systems.
- (3) System personnel perform their impact analyses cooperatively with the Process Manager managing progress for each system, creating a functional safety process for a whole vehicle with coordinated functional safety requirements. This has made it easier to identify omissions and oversights in the assignment of functional safety requirements.

References

- (1) ISO 26262: Road Vehicles—Functional Safety--, (2011)
- (2) Sagami, H., Hironaka, S., Mori, R., Mukai, T.: System Design Process in Compliance with ISO26262 Using Model-Based Design, Honda R&D Technical Review, Vol. 26, No. 2, p.173-180

APPENDIX

An explanation of the terms used in this paper as taken from functional safety standard ISO 26262 is given below:

- (1) Item
System or array of systems to implement a function at the vehicle level
- (2) Hazard
Potential source of physical injury or damage to human health caused by malfunctioning behavior of the item
- (3) ASIL
Automotive Safety Integrity Level. The levels are A, B, C, and D, with ASIL A representing the least stringent and ASIL D, the most stringent level.
- (4) QM
QM means the safety integrity level below ASIL A, and it denotes no requirement to comply with ISO 26262. The process for the items determined as QM is put under conventional quality management.

■ Author ■



Takashi OHTA



Hiroki SAGAMI