

Development of Configuration Management System for ISO26262

Hitoshi TAKUMI*

Yasuo KUROSAKI*

Hiroshi ISHIDA*

ABSTRACT

The functional safety standard ISO 26262 was published in November 2011. It is a functional safety standard for electrical and/or electronic systems within road vehicles. Compliance with this standard requires that the development process be defined and that numerous documents be created as proof that the development process has been implemented. The documents to be created in accordance with the development process were defined in advance and a configuration management system was developed to be capable of storing them together with the review results for each event during development. In order to realize traceability, a proprietary function was developed that automatically extracts items that are considered to require management for the purpose of functional safety from documents that are entered in predefined formats. This function is capable of displaying a list of the items, as well as a list of the definitions of the relations between items.

This system contributes to compliance with ISO 26262 and contains the increasing operational and administrative load.

1. Introduction

Recently there has been rising demand for increasingly advanced safety, environmental, comfort, and other such performance features in road vehicles. In order to satisfy this kind of demand, numerous electrical and/or electronic systems within road vehicles (in-vehicle E/E systems) are being installed. Assuring the safety of road vehicles will call for quality control of parts to prevent the outflow of faulty parts that may contribute to hazards and so that hazards themselves will not occur. In addition to this conceptual approach of intrinsic safety, it will also be necessary to conduct development by applying the conceptual approach of functional safety, whereby hazardous events that could occur are envisioned and reduced to acceptable risks by the function of safety devices and other systems that are designed to be fail-safe and fault-tolerant, thus assuring safety. The international standard that prescribes development procedures and requirement management during development for the purpose of applying this functional safety to products is the ISO 26262⁽¹⁾ functional safety standard.

ISO 26262 is based on international standard IEC 61508⁽²⁾ by the International Electrotechnical Commission (IEC), relating to the functional safety of electrical, electronic, and programmable electronic systems in processing and plant industry. Work on ISO 26262 standardization began in November 2005, and the standard was officially published on November 15, 2011.

In order to comply with ISO 26262, it will be necessary to perform the following kinds of operations for the configuration management for development of in-vehicle E/E system safety mechanisms.

First of all, development is initiated in accordance with the in-vehicle E/E system development process, and the configurations of documents (Work Product: WP) that are created by that activity are defined and managed. Second, the Automotive Safety Integrity Level (ASIL) that indicates the risk level of hazardous events is configured as a system for development. The WP is subjected to audit and assessment in accordance with the ASIL, and those results and the WP are stored together. Third, in preparation for an impact analysis when changes are made, relations with design and test results related to functional safety requirements are defined and traceability is enabled. Finally, the created WP is subjected to revision management, and when a change is made to the WP, the range of impact due to the change is specified and the approval of an appropriate manager is sought for the substance of the change and the reason(s) for it.

Honda began supporting ISO 26262 in 2008, and conventional in-vehicle E/E system development already took functional safety into account. Concepts are brought to maturity, however, by repeated meetings between the people in charge when development concepts are being considered. Consequently, estimations of the range of impact of changes and the number of iterations of audit and assessment of the content of changes are increasing. Furthermore, ISO

* Automobile R&D Center

26262 requires WP configured with traceability, and there is concern that this will further increase the operational and administrative load.

A system that would be capable of readily implementing configuration management and traceability therefore became necessary as a means of complying with ISO 26262 while also holding down the increase in development man-hours to a minimum.

2. Support for ISO 26262

2.1. Overview of ISO 26262

ISO 26262 is made up of 10 parts, from Part 1 to Part 10. It is configured as a standard for the entire lifecycle, from development and production of road vehicle in-vehicle E/E system to service (Fig. 1).

The content of these parts is as shown below.

Part 1 contains definitions of vocabulary and Part 2 contains requirements for corporate culture (safety culture) and company organization for the purpose of implementing functional safety activities as part of functional safety management.

Part 3 to Part 7 contain a systematic presentation of requirements for the corporate divisions that implement functional safety activities.

Development divisions of vehicle manufacturers have charge of the concept design specified in Part 3. Part 3 establishes Safety Goals for reducing risk to the level of what is acceptable as functional safety or lower. In terms of development results, it specifies that the appropriateness of safety goals be validated. It also defines the Functional Safety Requirements (FSR) that are required in order

to achieve the safety goals, and it also provides that development results be verified.

Working from that content, the development divisions or suppliers are in charge of the system development specified in Part 4. Part 4 specifies that the FSR presented in Part 3 are to be elaborated in greater detail, Technical Safety Requirements (TSR) are to be designed, and development results are to be verified.

Similarly, more detailed requirements are elaborated for hardware design in Part 5 and software design in Part 6. They also specify that development results are to be verified.

For production and operations, Part 7 specifies content that the production division and service division are to be in charge of.

Part 8 specifies supporting processes relating to functional safety development as a whole. These include management of requirements for functional safety as well as management of traceability, configuration management of documents, software libraries to be reused, and qualification of tools.

Part 9 defines the methods for implementing ASIL decomposition and the requirements involved in its implementation as ASIL-oriented and safety-oriented analysis.

Part 10 presents guidelines for the application of ISO 26262.

2.2. Definition of ASIL

Functional safety necessitates the assumption of hazardous events. In order to define the level of risk of a hazardous event, the frequency of occurrence of the

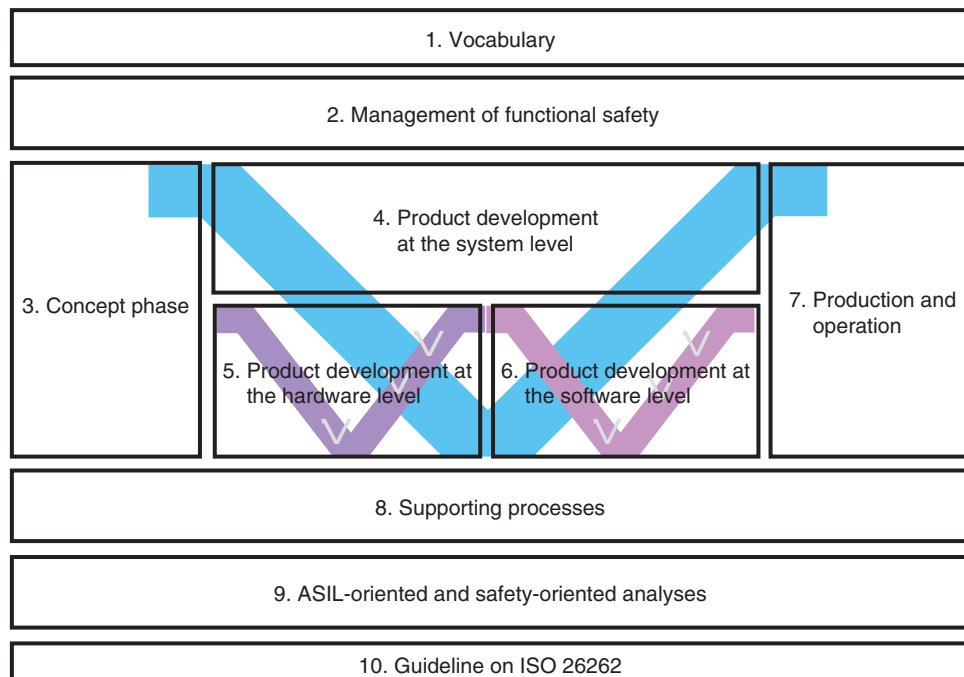


Fig. 1 Overview of functional safety standard

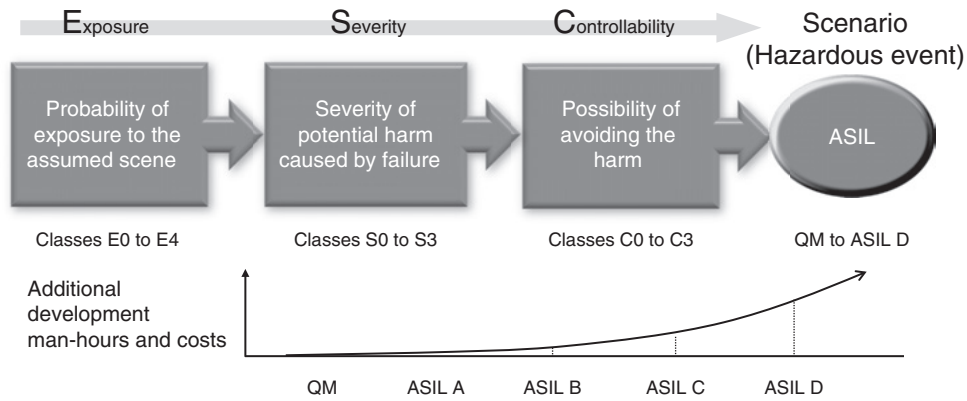


Fig. 2 Definition of ASIL and development cost

hazardous event (Exposure), the severity of harm to human beings caused if the hazardous event occurs (Severity), and the probability of whether human beings can take evasive action if the hazardous event occurs (Controllability) are used.

The three parameters (exposure, severity, and controllability) shown in Fig. 2 are estimated. They are then checked against a table defined in ISO 26262 to determine the ASIL for each assumed scenario. The ASIL is expressed by the letters A to D, where D is defined as the highest risk level.

The number of iterations of audit and assessment of the WP created, and the conditions regarding the approver, are set forth in accordance with the ASIL.

3. System Development Policy

Data management applications for the purpose of complying with ISO 26262 are already available on the market from software development companies.

The applications from the various companies were evaluated in terms of the reduction of man-hours.

No applications that satisfy Honda's requirements for configuring traceability and operability were found. The decision was therefore made to develop a proprietary system.

Analysis of ISO 26262 was carried out during development, and the following items for achievement were formulated.

(Item 1) The system is to be capable of defining the development process, revision management of the created WP is to be possible, and the WP is to be shareable between projects.

(Item 2) It is to be capable of extracting requirements and related items from within Microsoft Office documents, setting up the relations between the extracted items, and displaying those relations in list form.

(Item 3) It is to be capable of operations to upload the WP in a simple manner, of assisting with audits and assessments in the system, and of managing the results.

(Item 4) Requirements and WP are to be easily exchanged with suppliers.

The technical issues involved in incorporating these four items into a system were defined and system development was carried out.

4. System Development Headings

4.1. Configuration Management

Achieving the configuration management specified in Part 8 of ISO 26262 requires that management of the development process, configuration management of the WP, Change Management, and traceability be configured.

Conceptual database design was conducted of a database to implement the above content during in-vehicle E/E system development work and to record the management content.

Configuration management first involved definition of the function under development (Project), the development process (Process), and the scheduled product (Work Product Box: WPBox) to be created as the result from implementation of that development process. These were configured so that they could be recorded in the database.

Traceability was defined as management of the relationship (Relation) with the item subject to management (Object) that was extracted from the WP (Fig. 3).

The next phase was Process Management. This involved enabling the establishment of status, which indicates the state of progress, and of schedule, which includes the date of work commencement, the date of completion, and other such attributes individually for the Project, the Process, and the WPBox.

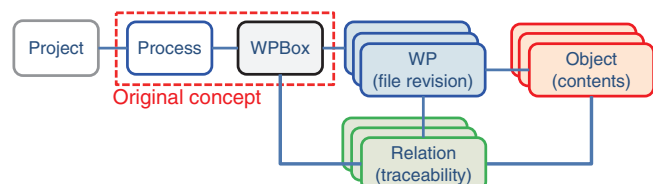


Fig. 3 Concept of configuration management

The final phase was Change Management. In order to preserve the results from verification of the development results, this involved defining the scheduled audits and assessments in the system as verification meetings (Events), so that the WPBox could be configured as an object of verification. When an Event was implemented, the revision number of the WP that was to be subject to audit and assessment was registered for the WPBox. The system was configured to enable implementation of an approval process (Approval Flow) that was in accordance with the ASIL of the function under development.

The WP that was finalized in accordance with the Approval Flow was used as a Baseline for when changes would be implemented. When development was completed and the transition to mass production was to be made, this could be treated as a Safety Case (Fig. 4).

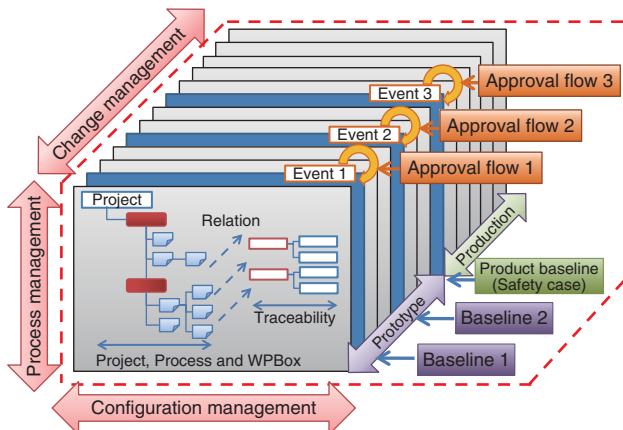


Fig. 4 Concept of data management

4.1.1. Tree structure and revision management

Under ISO 26262, it is necessary to simultaneously manage the development process and the WP created as a result.

This content was represented by a tree structure. A node on the tree was defined as a Process, and a leaf that is created under a node was defined as a WPBox.

The tree structure with the Process and WPBox created for each Project on the system was configured so that additions, changes, and deletions could be made. The tree structure was also configured so that its history could be managed (Fig. 5).

The WP uploaded in a WPBox is automatically assigned a control number in the order of uploading. The WP is identified by this number.

In this way, even if the same WP is uploaded multiple times, it will not be overwritten within the system. The control number can be used to conduct revision management. When designers want to refer to a past WP, they can specify its control number to view it.

4.1.2. Set carry-over

A function called set carry-over was developed for when the parts of an already developed E/E system are to be changed and used for the development of a similar E/E system. Set carry-over is a function that refers to the WPBox of the source project from the project that is to be partially changed.

When the WP in the already developed WPBox (the carry-over source) is changed using this function, the most up-to-date WP is also automatically made available

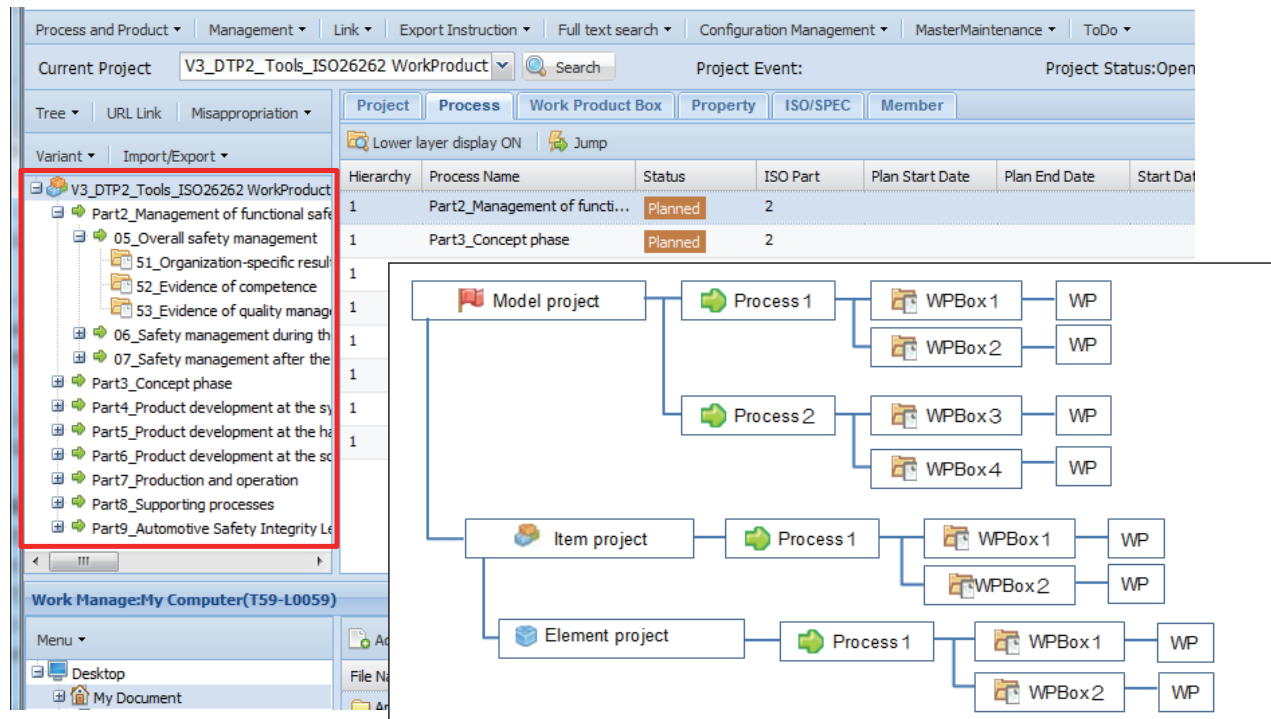


Fig. 5 Project tree, process and WPBox

for reference in the WPBox (the carry-over target) of the project that is to be partially changed.

When there is no desire to adopt the content of the most up-to-date changes or when there is a desire to add unique changes with no reference, a new WP can be uploaded in the carry-over target WPBox. This will automatically cancel the relationship with the WPBox in the carry-over source, allowing the development to proceed.

When set carry-over is executed, a Relation is set up between the WPBoxes in the carry-over target and the carry-over source. This enables traceability. They can therefore be handled as objects for calculation of impact, to be discussed later, and the man-hours involved in design changes can be reduced.

4.2. Traceability

Achieving the traceability sought in ISO 26262 requires more than establishing Relations with WPs. It also necessitates establishing the relations with requirements and test results themselves that are contained within a WP so that they can be tracked.

Relations of requirements can be set up by hierarchization of the control number assigned to the requirement when elaborating the detail of the requirement in accordance with the development process.

Items to be tested to verify the design content can be subjected to stand-alone testing, unit testing, inter-function linked testing, and so on. Since the testing is conducted in phases and the test items are aggregated, a control number is assigned for each phase of the testing and the relations between numbers are set up according to aggregation.

In order to verify whether the requirements for functional safety have been achieved, it is necessary to configure traceability between requirements and test items (Fig. 6).

A function was developed that can extract the requirements and test items from the WP uploaded in the system, set up the relations, and display the content in list form.

4.2.1. Extraction of items from within documents

The WP containing notations of safety goals and FSR to be achieved is published as a specification form and the information is transmitted to related Honda divisions and suppliers.

Templates for specification forms containing notations of items involved in complying with ISO 26262 are created as Microsoft Office documents. The system was configured so that those templates can be analyzed using Office Open XML, which is published by Microsoft, and the Objects can be extracted from XML tag names and recorded content (Fig. 7).

The hierarchical structure of Objects expressed in templates can also be extracted. The system is configured so they can be registered and stored in the database.

4.2.2. Conceptual approach of the Relation

In this system, configuration management involves defining the Process and WPBox. Revision management is carried out on the WP that is uploaded in the WPBox [Fig. 8(1)].

When the WP has been uploaded, the system automatically adds a Relation between the WPs according to the Relation between WPBoxes [Fig. 8(2)].

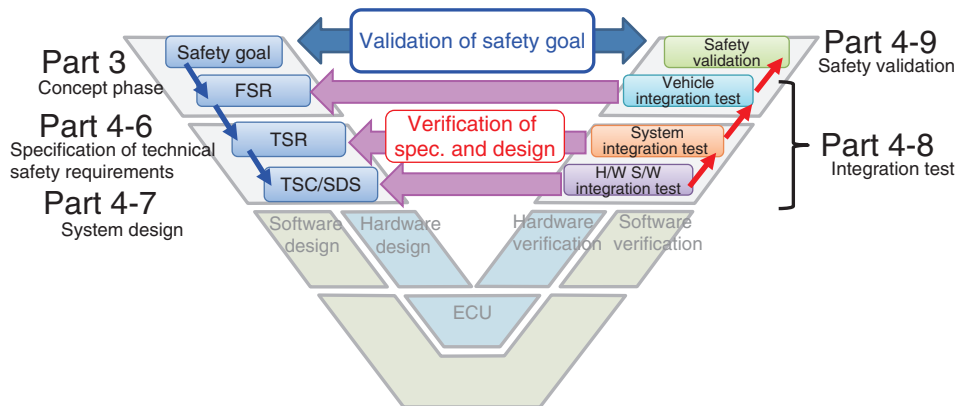


Fig. 6 Verification and validation in ISO 26262

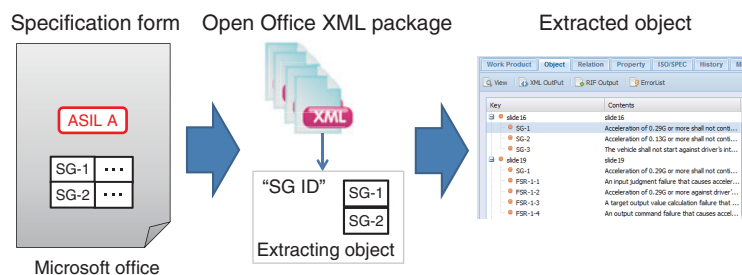


Fig. 7 Extracting object from Microsoft office

When a WP that has been changed is uploaded in a WPBox by means of revision management within WPBoxes, this allows a Relation between WPs that was set up before the change to continue with the same setting after the change [Fig. 8(3)].

It is also a distinctive feature of this function that when setting up a Relation, the kind and direction can also be set up.

Depending upon the direction set up in the Relation, it can represent the relationship of referencing between Objects or the relationship of being referenced. By setting the kind of Relation, the meaning of the relationship can be represented (Fig. 9).

4.2.3. Calculation of the range of impact

When requirements are changed, it is necessary to

search the related design content and test results and to specify the range of impact of the change.

In this system, the set up Relations are traced in order and the related items are displayed in a hierarchical structure. This allow the range of the impact to be clearly indicated (Fig. 10).

The kind and direction of the Relation and the depth of the hierarchical structure can be set up as search conditions. When the range of impact is specified, the search results can be further focused. The search conditions can be reset for items displayed as search results so that a series of calculations of the range of impact can be performed consecutively. This can be used as a measure to increase the efficiency of search operations during development.

As shown in Fig. 11, a form can also be created to

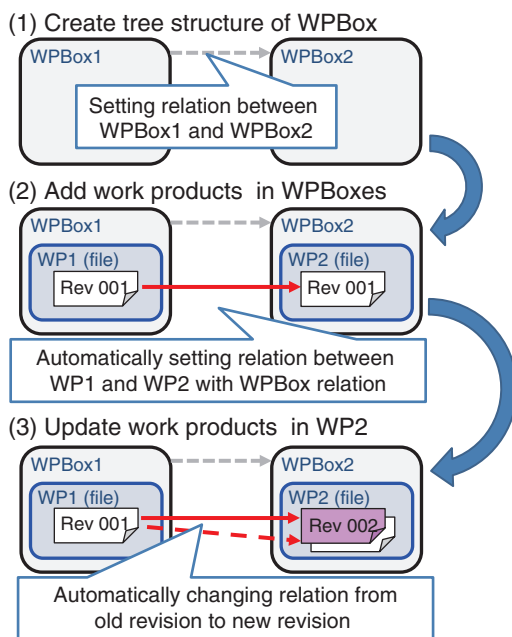


Fig. 8 Automatically setting a Relation

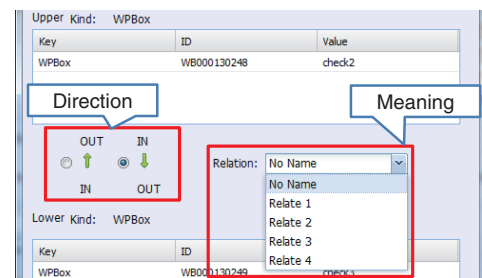


Fig. 9 Setting direction and meaning of a Relation

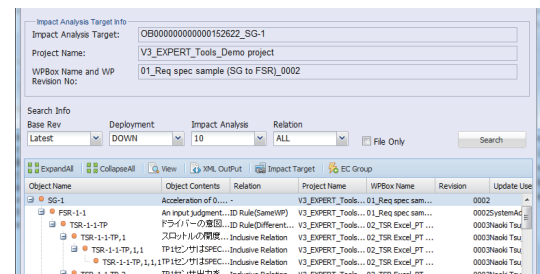


Fig. 10 Results of impact analysis

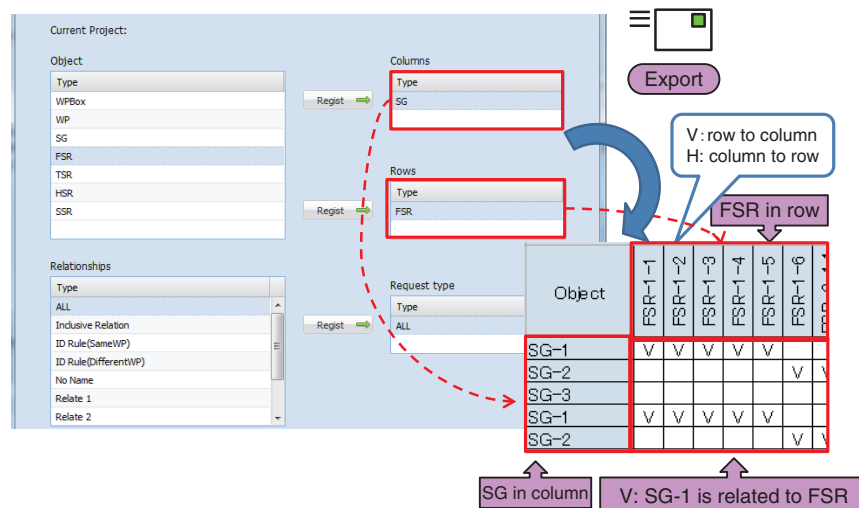


Fig. 11 Matrix of objects and Relations

specify items selected from among the extracted items to be displayed along vertical and horizontal axes, and to specify the kind of Relation set up among those items and cross-tabulate them. This form can be used to check whether any relationships have been omitted from set up.

4.3. Usability

It is necessary to be able to reference and upload documents without installing any special applications. The ability to run on a web browser was therefore made a system requirement.

Rich Internet Application (RIA) technology and the Extjs Javascript library were adopted in order to enhance usability on web browsers. This has enabled the use of drag-and-drop in web browsers, and achieved more intuitive

operation when uploading documents and setting up relations (Fig. 12).

4.4. Supplier Coordination and Collaboration

In order to comply with ISO 26262, a vehicle manufacturer needs to transmit its requirements accurately to the parts suppliers. The suppliers to which requirements have been transmitted must design functions to achieve the requirements and present the design results to the vehicle manufacturer as a WP. Since these operations of requirements, design content, and test results have to be configured for traceability, a function for data exchange between the vehicle manufacturer and suppliers was developed (Fig. 13).

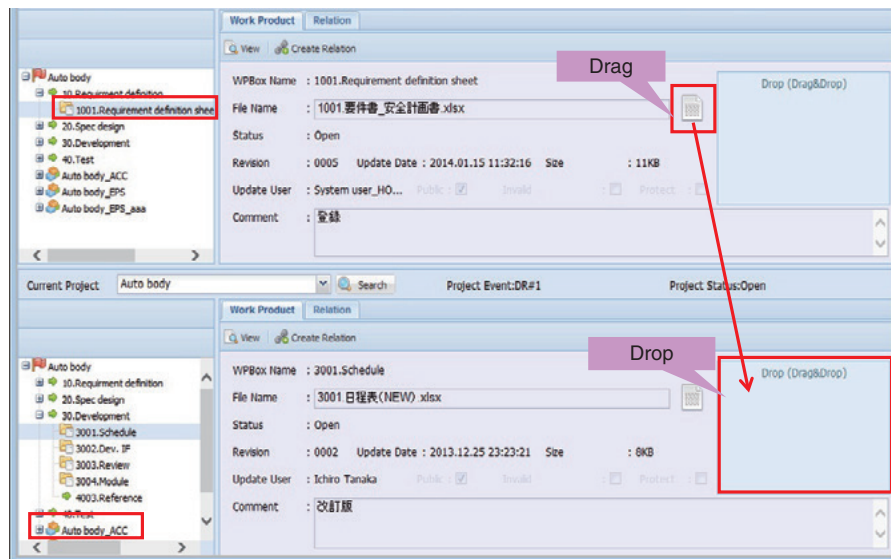


Fig. 12 Setting relations with drag and drop operation

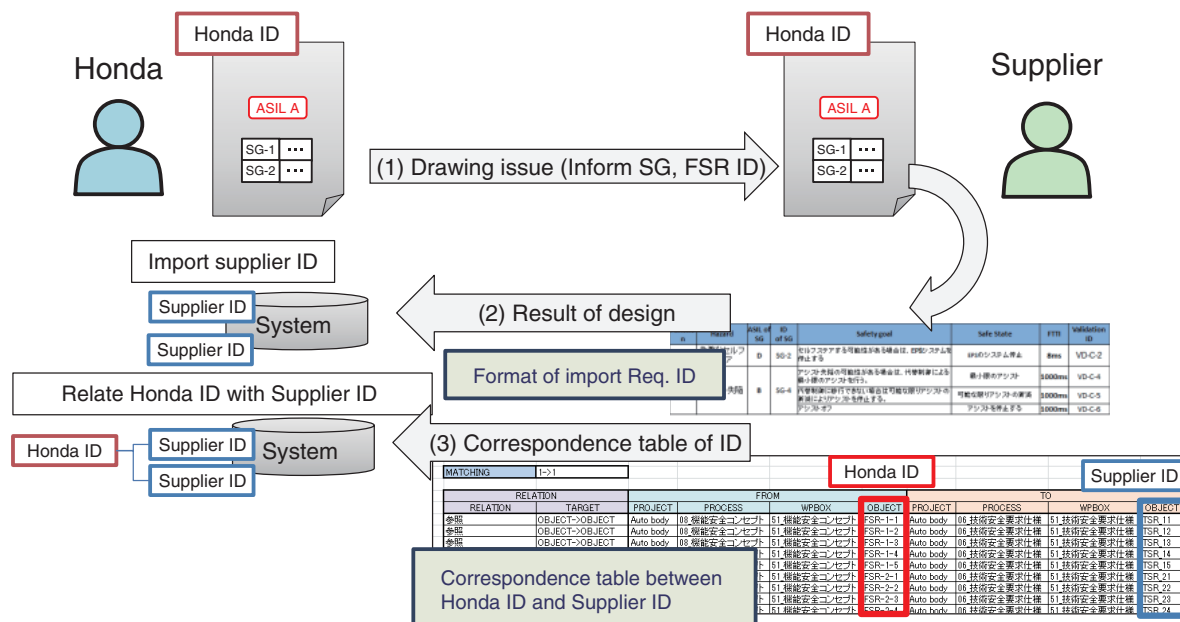


Fig. 13 Data exchange between Honda and suppliers

4.4.1. RIF output of requirements

The Requirements Interchange Format (RIF) is a format devised for the exchange of requirements between enterprises. It was created by an organization called the Hersteller Initiative Software (HIS)⁽³⁾, which is made up of five companies: Audi, BMW, Daimler, Porsche, and Volkswagen.

The RIF format has been adopted by commercially available applications for managing requirements. In order to convey requirements to suppliers, this format must be supported.

The system was therefore configured so that the requirements contained in specification forms could be extracted and the content stored in the database could be output in a format (XML file) that complies with RIF.

However, the commercially available applications that support RIF differ in the content they include in their RIF format. This makes a conversion operation necessary when exchanging data (Fig. 14).

4.4.2. Importing and exporting of configuration management content

Under ISO 26262, a WP that complies with the standard has to be put together and stored when the development has been completed. Since the stored WP is used as the Baseline when design changes are made, it needs to be capable of restoration at any time.

It is considered desirable to exchange not just functional safety information with suppliers, but also information

required for development of functions, so as to heighten the efficiency of development operations.

In order to achieve these objectives, a function was developed to enable import and export both of tree structures created in configuration management and of WP with specified revision numbers.

This function was configured to confirm whether any items transmitted to suppliers or confidential items are included by providing the output for export in accordance with the Approval Flow set up in the system (Fig. 15).

The function was configured to reflect WP import after confirming the impact on configuration information in the system (Fig. 16). Data that can be imported is basically assumed to be XML data output from the system. However,

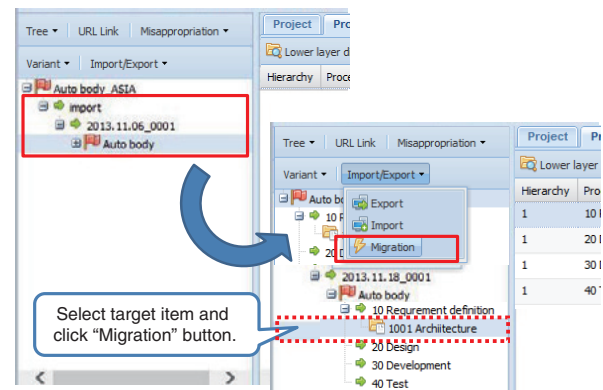


Fig. 16 Import operation

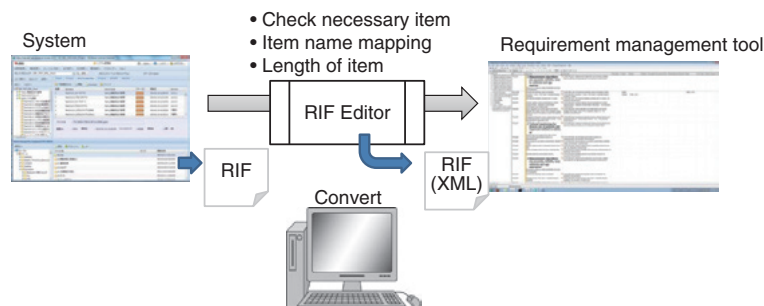


Fig. 14 Convert RIF format for exchange

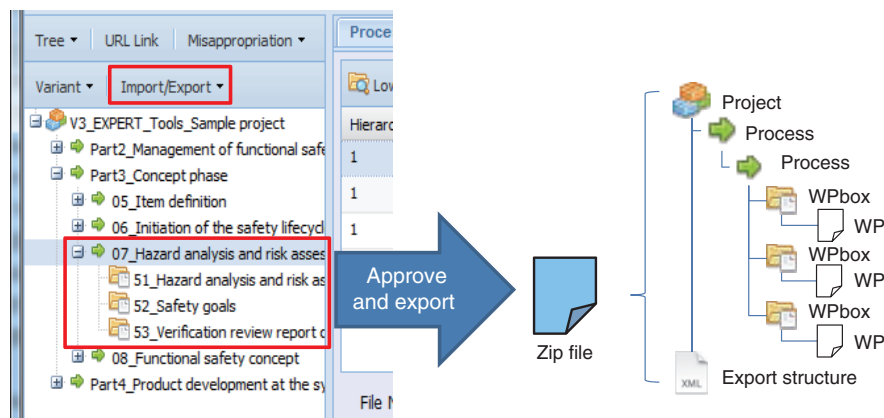


Fig. 15 Export operation

XML data output from other tools can be converted for use by this system so that import is possible.

5. Conclusion

Development of the system described above yielded the following:

- (1) Development processes and WP that are compliant with ISO 26262 can be defined in the system.
- (2) Traceability was achieved by automatically extracting requirements from registered WP and defining Relations between requirements.
- (3) Verification meetings in the course of development can be defined in the system as Events, and product and verification results can be retained in storage.
- (4) By displaying the Relations between configured items in list form, the system became capable of identifying the range of impact and reducing man-hours spent on search.

References

- (1) ISO 26262 : Road Vehicles – Functional Safety (2011)
- (2) IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (2000)
- (3) <http://www.automotive-his.de/rif/> 2014/4/14

■ Author ■



Hitoshi TAKUMI



Yasuo KUROSAKI



Hiroshi ISHIDA