

ISO26262 準拠のための構成管理システム構築

Development of Configuration Management System for ISO26262

宅 美 仁 史*
Hitoshi TAKUMI

黒 崎 泰 央*
Yasuo KUROSAKI

石 田 宏 司*
Hiroshi ISHIDA

要 旨

2011 年 11 月に機能安全規格 (ISO26262) が発行された。この規格は車載電子制御システムに関する機能安全規格である。規格に準拠するためには、開発プロセスを定義し、開発プロセスを実施した証拠として多くのドキュメントを作成する必要がある。開発プロセスに従って作成されるドキュメントを事前に定義でき、開発中のイベントごとにレビュー結果と共に保管できる構成管理システムを構築した。また、トレーサビリティを実現するために、あらかじめ定義した書式で記述されたドキュメントから、機能安全で管理が必要とされる項目を自動抽出し、項目間の関連の定義と項目を一覧表示できる機能を独自開発した。

本システムにより、ISO26262 への準拠および業務負荷の増加を抑制することが可能となった。

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. はじめに

近年の自動車においては、安全、環境、快適などの各性能に対し高度な要求があり、これらを満足するために数多くの車載電子制御システムが搭載されている。自動車の安全を確保するために、部品の品質管理によって危険につながる不具合部品の流出を防止し、危険そのものが起こらないようにする考え方 (本質安全) に加えて、起こり得る危険事象を想定し、フェイルセーフ設計、フォールトトレラント設計された安全装置等の機能によって許容できるリスクまでに低減させ、安全性を確保する考え方 (機能安全) を適用し開発をおこなう必要がある。この機能安全を製品に適用するために、開発時の要求管理や開発手順を規定した国際規格が機能安全規格 (ISO26262) ⁽¹⁾ になる。

ISO26262 は、国際電気標準会議 (IEC) によるプロセスやプラント産業における電気、電子、プログラマブル電子の機能安全に関する国際規格 IEC61508⁽²⁾ を基本とし、2005 年 11 月より規格化が開始され、2011 年 11 月 15 日に正式発行された。

ISO26262 に準拠するためには、車載電子制御システムの安全機構の開発において、構成管理として以下のような作業の実施が必要となる。

はじめに、車載電子制御システムの開発プロセスに従って開発を開始し、その活動によって作成されるドキュメント成果物 (Work product: WP) の構成を定義し、管理する。次に、危険事象のリスクレベルを表す Automotive Safety Integrity Level (ASIL) を開発対象システムに設定する。ASIL に従って、成果物の監査、査定を実施し、その結果と

* 四輪 R&D センター

共に成果物を保管する。三つめとして、影響分析に備えて、機能安全の要求事項に関係する設計、テスト結果に関連を定義し、トレーサビリティを可能にする。最後に、作成された成果物を版管理し、成果物の変更をおこなう際には、変更による影響範囲を特定し、適切な管理者による変更内容と変更理由の承認を実施する。

弊社では 2008 年より ISO26262 の対応を開始しており、従来の車載電子制御システム開発において、既に機能安全は考慮されている。ただ、開発コンセプトの検討の際に、担当者間で打ち合わせを重ねることによってコンセプトを成熟させていくため、変更による影響範囲の算出および変更内容の監査、査定回数が増大している。加えて、ISO26262 が要求する成果物にトレーサビリティを設定する必要がある、さらに業務負荷が増大することが懸念されている。

そのため、ISO26262 に準拠しながら、開発工数の増加を最小に抑える取り組みとして、構成管理とトレーサビリティを容易に実施できるシステムが必要となった。

2. ISO26262 準拠対応

2.1. ISO26262 の概要

ISO26262 は、Part1 から Part10 の 10 章で構成されており、車載電子制御システムの開発から生産、サービスに至るまでのライフサイクル全体に対しての規格で構成されている (Fig. 1)。

各 Part の内容は以下のとおりである。

Part1 は用語の定義、Part2 は機能安全管理として機能安全活動を実施するための企業文化 (安全文化)、会社組織

に対する要求が記述されている。

Part3 から Part7 においては、機能安全活動を実施する部門への要求事項が体系的に記述されている。

自動車メーカの開発部門は Part3 で規定されているコンセプト設計を担当する。Part3 では、機能安全として許容できるリスク以下に低減させる安全目標 (Safety Goal) を設定し、開発結果として、安全目標が妥当かどうかを確認することが規定されている。また、安全目標を実現するための要求事項である機能安全要求 (Functional Safety Requirement :FSR) を定義し、あわせて開発結果を検証することが規定されている。

その内容を受け、開発部門またはサプライヤが Part4 で規定されるシステム開発を担当する。Part4 では、Part3 で提示された FSR を詳細化し、技術安全要求 (Technical Safety Requirement:TSR) を設計し、開発結果を検証することが規定されている。

同様に、Part5 のハード設計、Part6 のソフト設計では要求事項がそれぞれ詳細化され、開発結果の検証が規定されている。

Part7 の生産と運用では、生産部門およびサービス部門が担当する内容が規定されている。

Part8 は機能安全開発全体に関わる支援業務として、機能安全の要求事項の管理およびトレーサビリティ管理、ドキュメントの構成管理規定、再利用されるソフトウェアライブラリやツールの認定について規定されている。

Part9 は ASIL 指向と安全指向の分析として、ASIL の分解の実施方法と実施にあたっての要件が定義されている。

Part10 は規格適用のためのガイドラインが記載されている。

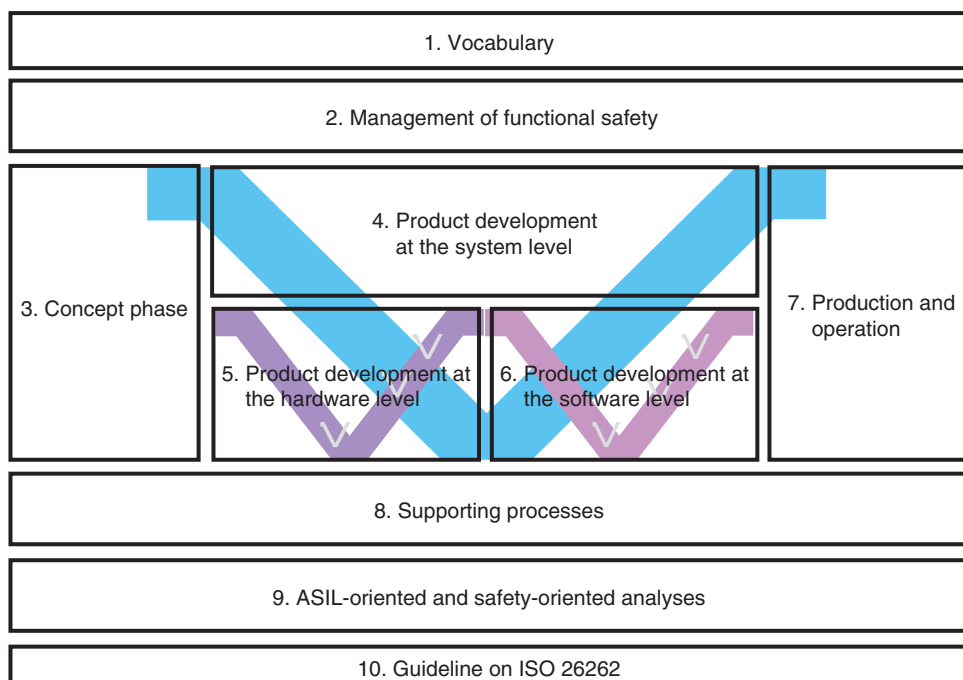


Fig. 1 Overview of functional safety standard

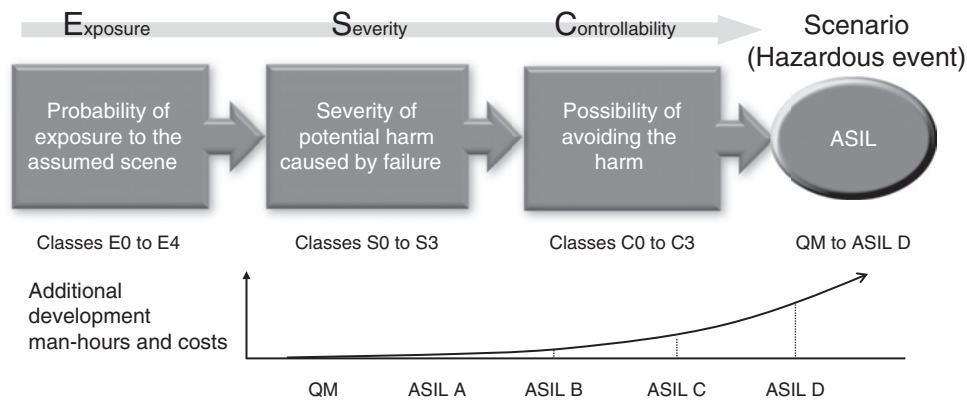


Fig. 2 Definition of ASIL and development cost

2.2. ASIL の定義

機能安全には、危険事象の想定が必要となる。危険事象のリスクのレベルを定義するためには、その危険事象が起こる頻度 (Exposure)、危険事象が起こった場合の人に対する危害度 (Severity)、危険事象が起きた場合に人が回避動作をとれるかどうかの確率 (Controllability) を用いる。

Fig. 2 で示す三つの指標値 (Exposure, Severity, Controllability) を見積もり、ISO26262 で定義されているテーブルに照らし合わせて、想定される ASIL を決定する。ASIL はアルファベットの A から D で表現され、D が一番高いリスクレベルと定義される。

ASIL に従って、作成された成果物の監査、査定の回数や承認者の条件が設定される。

3. システム開発方針

ISO26262 に準拠するためのデータ管理アプリケーションは、ソフトウェア開発会社から既に市販されている。

工数削減の観点から各社のアプリケーションを評価した。

トレーサビリティ設定や操作性において弊社の要求を満たすものは見つからなかったため、独自システムを開発することとした。

開発に際して、ISO26262 を解析し、以下の達成項目を設定した。

(項目 1) 開発プロセスをシステムに定義でき、作成された成果物の版管理が可能で、プロジェクト間で成果物を共用できること

(項目 2) Microsoft 社の Office 文書から要求事項等の項目を抽出し、抽出された項目間に関連を設定し、その関連を一覧表示できること

(項目 3) 成果物の登録操作が簡単にでき、システム上で監査、査定の補助をおこない、結果を管理できること

(項目 4) 取引先と要求事項や成果物を簡単に交換できること

四つの項目をシステム化するにあたって技術課題を設定し、システム開発をおこなった。

4. システム開発項目について

4.1. 構成管理

ISO26262 の Part8 に規定されている構成管理を実現するためには、開発プロセスの管理、成果物の構成管理、変更管理およびトレーサビリティの確立が必要となる。

上記内容を車載電子制御システムの開発作業中に実施し、管理内容を記録するため、データベースの概念設計を実施した。

まず、構成管理 (Configuration Management) として、開発機能対象 (Project)、開発プロセス (Process) とその開発プロセスの実施結果として作成される予定成果物 (Work Product Box: WPBox) を定義し、データベースへ記録できるようにした。

トレーサビリティとしては、成果物から抽出される管理対象項目 (Object) との関係 (Relation) を管理するように定義した (Fig. 3)。

次に、プロセス管理 (Process Management) として Project, Process および WPBox それぞれに、進行状況を示すステータスや作業開始日付や完了日付等のスケジュールを設定することができるようにした。

最後に、変更管理 (Change Management) として、開発結果を検証した結果を保存するため、監査、査定予定を検証会 (Event) としてシステムに定義し、検証対象となる WPBox を設定できるようにした。検証会実施時には、

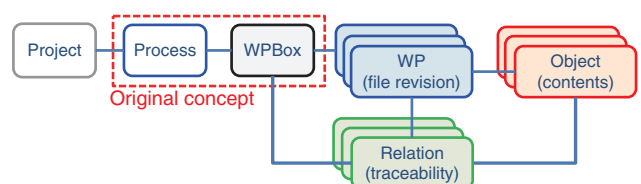


Fig. 3 Concept of configuration management

WPBox に対し、監査、査定対象となる成果物の版番号を登録し、開発対象の ASIL に従った承認処理 (Approval Flow) を実施できるようにした。

承認処理によって確定された成果物は、変更を実施する際の基準 (Baseline) として利用され、開発を完了し量産に移行する場合には、セーフティケース (Safety Case) として扱うことができる (Fig. 4)。

4.1.1. ツリー構造と版管理

ISO26262 では、開発プロセスと結果として作成される成果物を合わせて管理することが必要になる。

この内容をツリー構造で表現し、ツリー上のノードを Process とし、ノード配下に作成されるリーフを WPBox と定義した。

システム上で Project 毎に作成された Process と WPBox のツリー構造の構成を追加、変更、削除できるよう

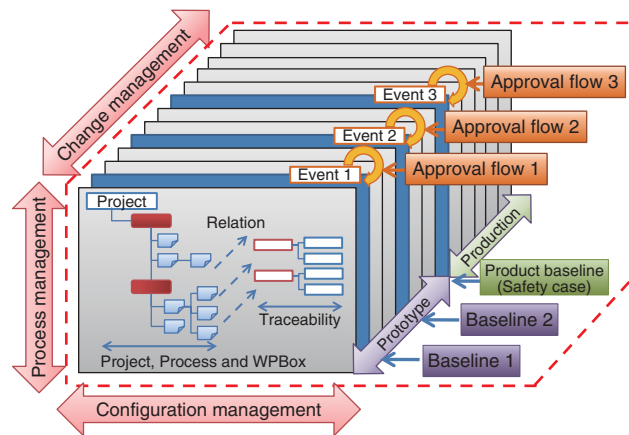


Fig. 4 Concept of data management

にし、ツリー構造の履歴を管理できるようにした (Fig. 5)。

WPBox に登録された成果物自体は、登録された順序で自動的に管理番号を採番識別される。

これにより、同じ成果物が複数回登録された場合でも、システム内部で上書きせず、管理番号を用いて版管理できる。設計者が過去の成果物を参照したい場合は、管理番号を指定して閲覧することができる。

4.1.2. 流用設定

既に開発がおこなわれているシステムを部分的に変更し類似機能の開発をおこなう場合がある。部分変更するプロジェクトから、元となるプロジェクトの WPBox を参照する機能 (流用設定) を開発した。

これにより、既に開発がおこなわれている WPBox (流用元) で成果物が更新されて登録された場合、部分変更するプロジェクトの WPBox (流用先) においても自動的に最新の成果物を参照できる。

最新の変更内容を採用したくない場合や、参照せずに独自の変更を加えたい場合には、流用先の WPBox に新規に成果物を登録することで、自動的に流用元の WPBox との関係を解除し開発を進めることができる。

流用設定を実行した際に、流用先と流用元の WPBox 間で Relation が設定され、トレーサビリティが可能となる。よって、後述する影響計算の対象として扱うことができ、設計変更時の工数削減が可能となる。

4.2. トレーサビリティ

ISO26262 で求められるトレーサビリティを実現するには、成果物の関連だけでなく、成果物の内部に記述された

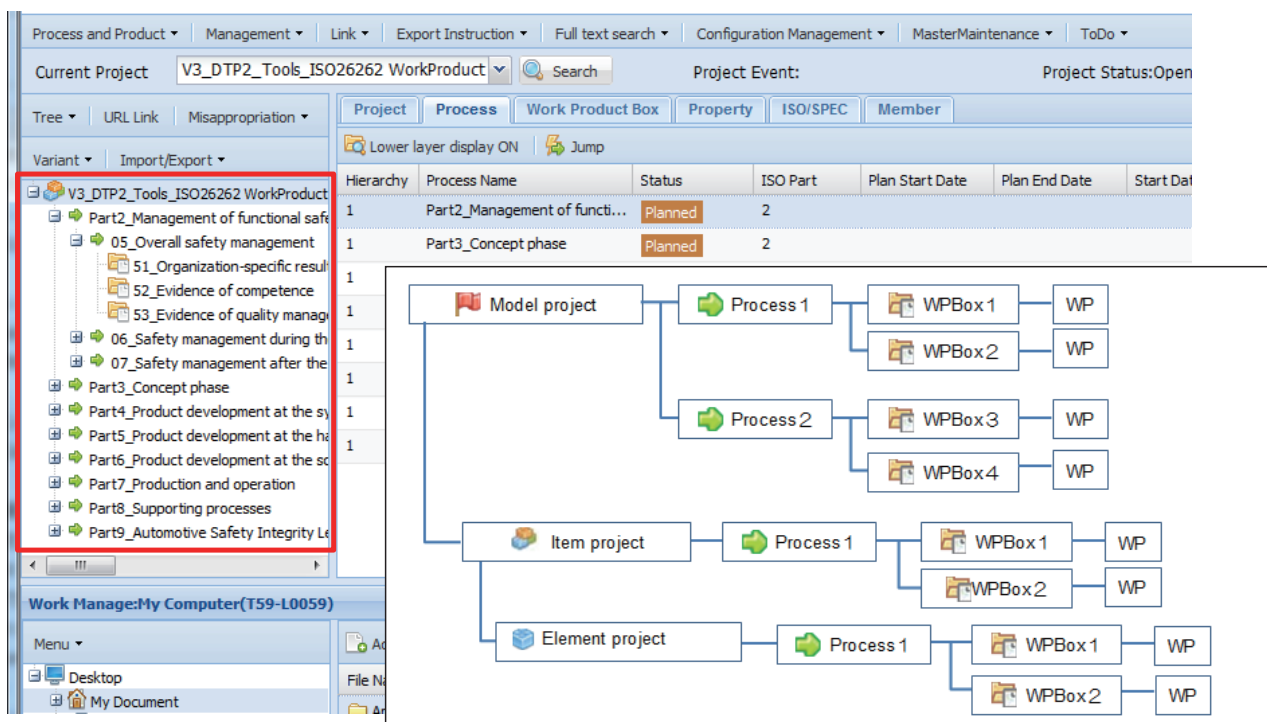


Fig. 5 Project tree, process and WPBox

要求事項やテスト結果そのものに対して関連を設定し、追跡できるようにする必要がある。

要求事項の関連については、開発プロセスに従って要求事項を詳細化する際に、要求項目に与える管理番号を階層化することで設定することが可能である。

また、設計内容を確認するテスト項目については、単体テストからユニットテスト、機能間の結合テスト等、段階的にテストが実施されテスト項目が集約されるため、テスト段階ごとに管理番号を与え集約に従って関連を設定する。

機能安全の要求事項が達成されているかどうかを検証するため要求事項とテスト項目との間にトレーサビリティを設定する必要がある (Fig. 6)。

システムに登録された成果物から要求事項およびテスト項目を抽出し、設定された Relation を一覧表示する機能を開発した。

4.2.1. ドキュメント内の項目抽出

達成すべき安全目標や FSR を記載した成果物を仕様書として発行し、弊社関係部門およびサプライヤに情報を伝達する。

ISO26262 に準拠するための項目が記載された仕様書のひな形を Microsoft 社の Office 文書で作成する。そのひな形を Microsoft 社で公開されている Office Open XML 形式で解析し、XML のタグ名と記載内容から Object を抽出できるようにした (Fig. 7)。

また、ひな形で表現されている Object の階層構造も抽出し、データベースへ登録することを可能とした。

4.2.2. リレーションの考え方

本システムでは、構成管理として、Process と WPBox を定義し、WPBox に登録される成果物が版管理される。

成果物間の関係が事前に確定している場合には、WPBox 間にあらかじめ Relation を設定できる [Fig. 8 (1)]。

成果物を登録した場合には、WPBox 間の Relation により、システムが自動的に成果物間に Relation を追加する [Fig. 8(2)]。

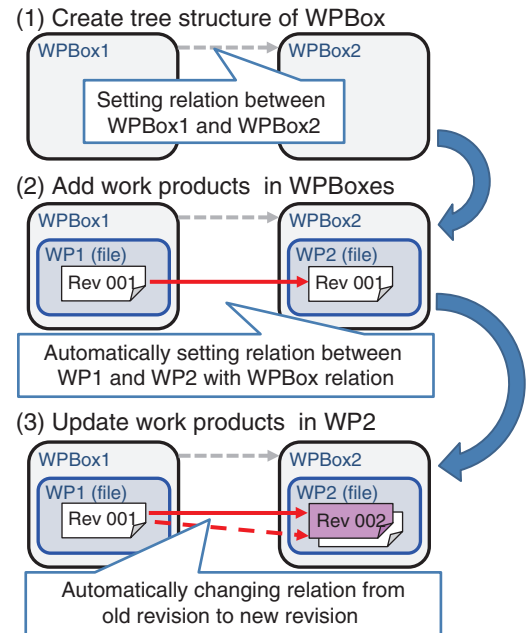


Fig. 8 Automatically setting a Relation

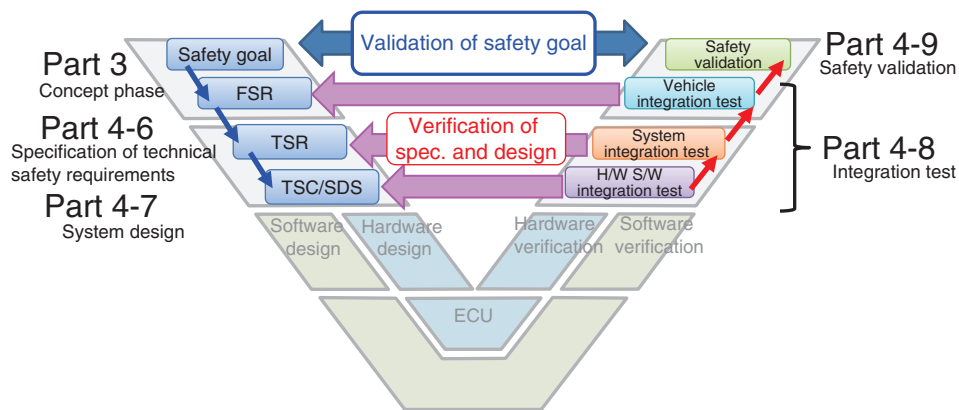


Fig. 6 Verification and validation in ISO 26262

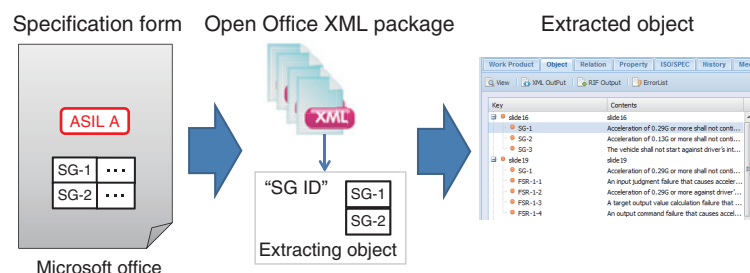


Fig. 7 Extracting object from Microsoft office

WPBox 内での版管理により, WPBox に成果物が変更されて登録された場合には, 変更前に設定されていた成果物間の Relation を変更後に引き継いで設定することが可能となる [Fig. 8(3)].

また, 本機能の特徴として, Relation を設定する際に, 方向と種類を設定できる。

Relation に設定された方向によって, Object 間の参照する関係や参照される関係を表現することができる。加えて Relation の種類を設定することで, 関係の意味を表現することができる (Fig. 9)。

4.2.3. 影響範囲の計算

要求項目を変更する場合, 関連する設計内容やテスト結果を検索し, 影響範囲を特定する必要がある。

本システムでは, 設定された Relation を順次たどり, 関連づけられた項目を階層構造で表示することで, 影響する範囲を明示することができる (Fig. 10)。

Relation の方向や種類, 階層構造の深さを検索条件として設定し, 影響範囲特定時の検索結果を絞り込むことができる。検索結果に表示された項目に対して, 検索条件を再度設定し, 連続して影響範囲の計算を実施することができ, 開発時の検索作業の効率化を図ることが可能となっている。

また, Fig. 11 で示すように抽出された項目の中から, 縦軸と横軸に表示させる項目と, それらの項目に設定されている Relation の種類を指定し, クロス集計した帳票を作成できる。この帳票により, 関連が漏れなく設定されているか確認することができる。

4.3. ユーザビリティ

特別なアプリケーションをインストールすることなくドキュメントを参照し, 登録することが必要なため, Web Browser で稼働することをシステム要件とした。

Web Browser 上での使い勝手 (ユーザビリティ) を向上させるため, Rich Internet Application (RIA) 技術として, Javascript ライブラリの Extjs を採用した。これにより Web Browser 内でのドラッグとドロップが可能となり, ドキュメント登録時や関連の設定時に直観的な操作を実現した (Fig. 12)。

4.4. サプライヤ連携

ISO26262 に準拠するためには, 自動車メーカーとしてサプライヤに要求事項を正確に伝達する必要がある。要求を伝達されたサプライヤは, 要求を実現する機能を設計し, 設計結果として成果物を自動車メーカーに提示する必要がある。

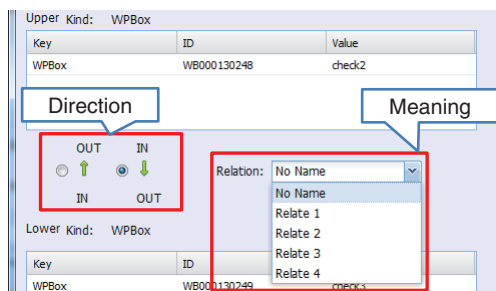


Fig. 9 Setting direction and meaning of a Relation

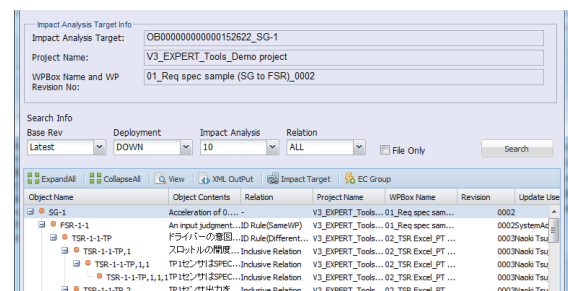


Fig. 10 Results of impact analysis

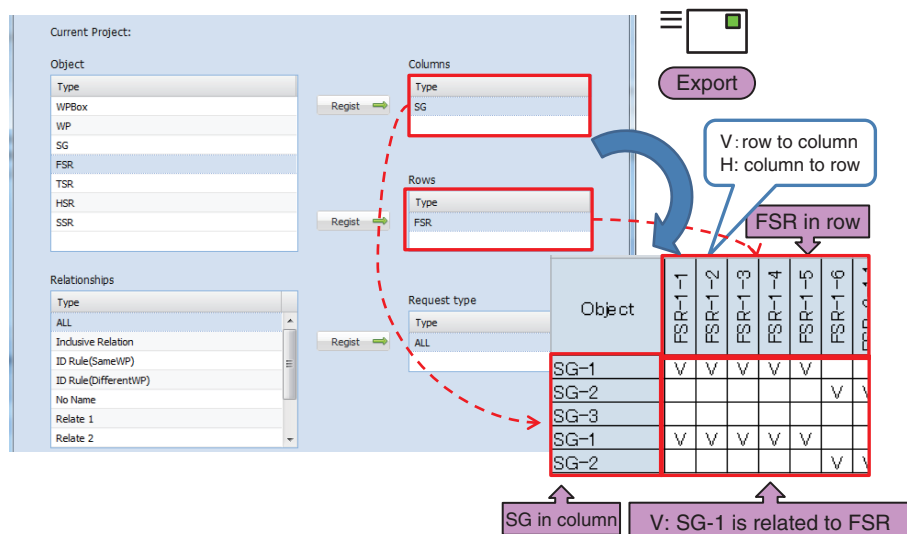


Fig. 11 Matrix of objects and Relations

る。これら要求事項と設計内容およびテスト結果はトレーサビリティの設定が必要であるため、自動車メーカとサプライヤ間でのデータ交換機能を開発した (Fig. 13)。

4.4.1. 要求項目の RIF 出力

Requirements Interchange Format (RIF) は要求事項を企業間で交換するためのフォーマットである。これは Audi, BMW, Daimler, Porsche, Volkswagen の 5 社で構成されている Hersteller Initiative Software (HIS) という組織によって作成された⁽³⁾。

このフォーマットは要求事項を管理する市販アプリケーションで採用されており、サプライヤに要求事項を伝えるためには RIF への対応が必要である。

そのため、仕様書に記載された要求項目を抽出し、データベースに登録された内容から、RIF に準拠したフォーマット (XML ファイル) で出力できるようにした。

ただし、RIF に対応している市販アプリケーションごとに RIF の記載内容に差異があるため、データ交換時に変換作業が必要である (Fig. 14)。

4.4.2. 構成管理内容のインポートおよびエクスポート

ISO26262 では規格準拠の成果物を開発完了時にまとめて保管する必要がある。保管された成果物は、設計変更時の基準として使用するため、任意のタイミングで復元できる必要がある。

また、機能安全だけでなく、機能開発に必要な情報をサ

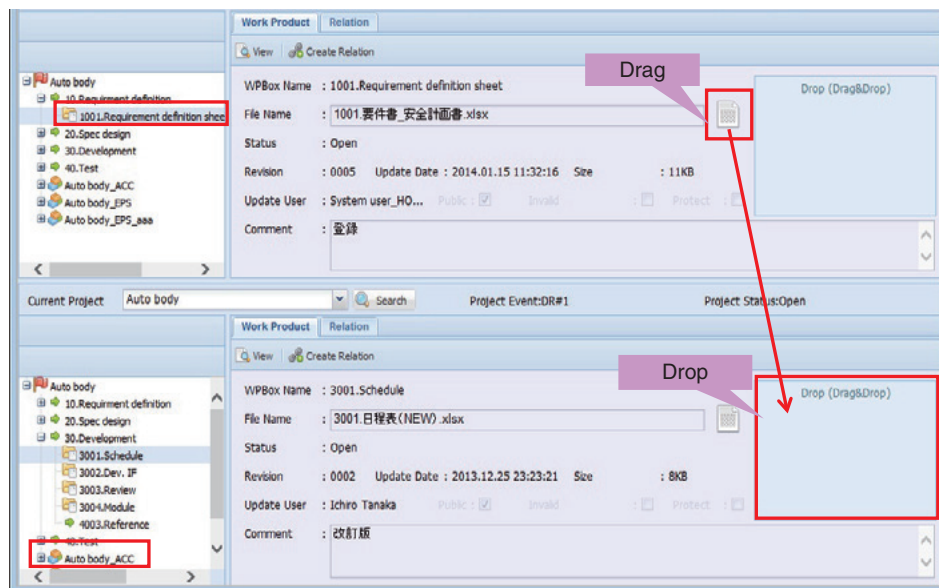
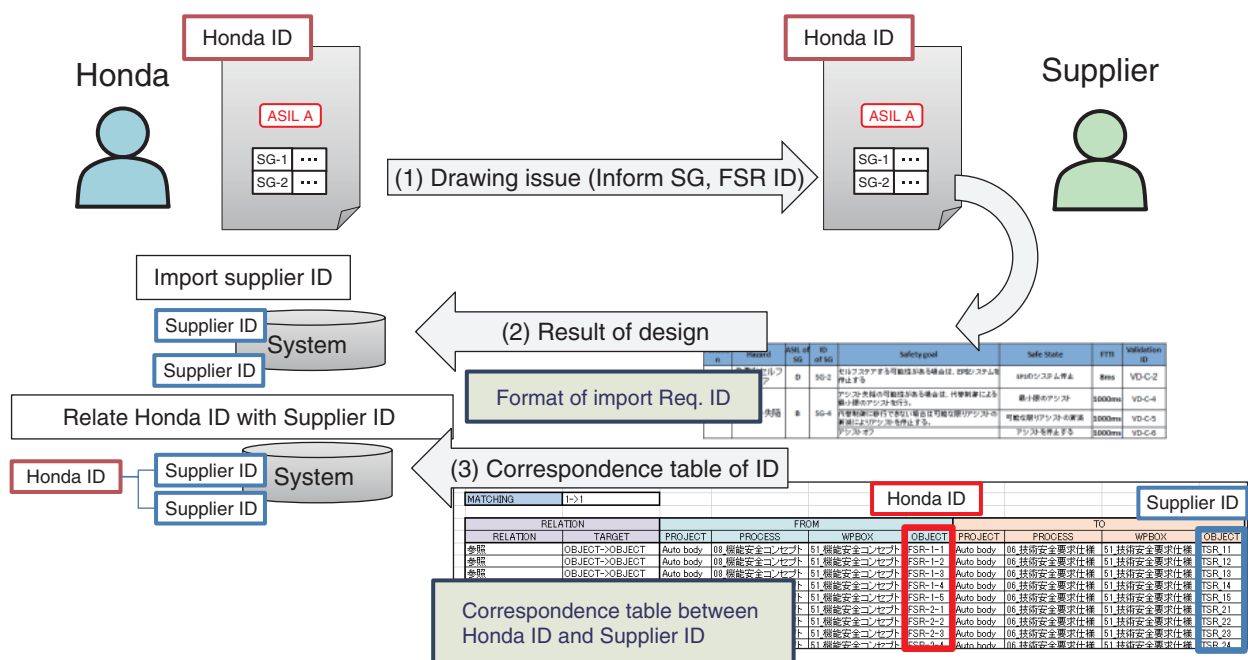


Fig. 12 Setting relations with drag and drop operation



プライヤと交換し、開発業務を効率化することが望ましい。

これらを実現するために、構成管理で作成したツリー構造と指定された版番号の成果物の両方をインポートおよびエクスポートできる機能を開発した。

サプライヤへの伝達事項や機密事項の有無を確認するため、システム上に設定された承認処理の後にエクスポートされる機能とした (Fig. 15)。

成果物のインポートに関しては、システム上の構成情報に対して、影響を確認してから反映する機能とした (Fig. 16)。インポートできるデータは基本的に本シス

テムから出力された XML データを想定しているが、他ツールから出力された XML を本システム用に変換することで、インポートが可能となる。

5. まとめ

上述のシステム開発により、

- (1) ISO26262 に準拠した開発プロセスおよび成果物をシステム上に定義できるようにした。
- (2) 登録された成果物から、自動的に要求項目を抽出し、

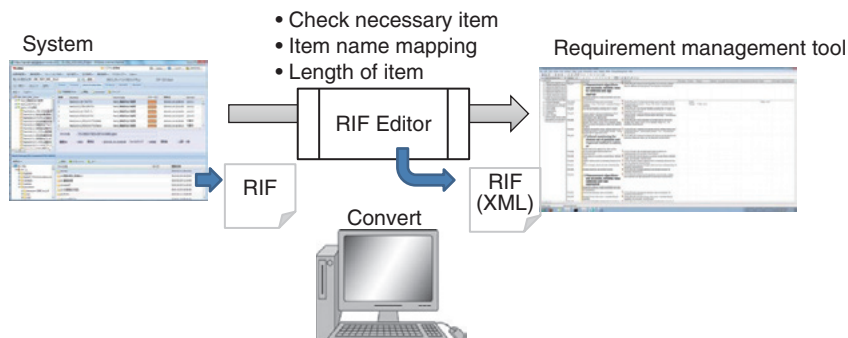


Fig. 14 Convert RIF format for exchange

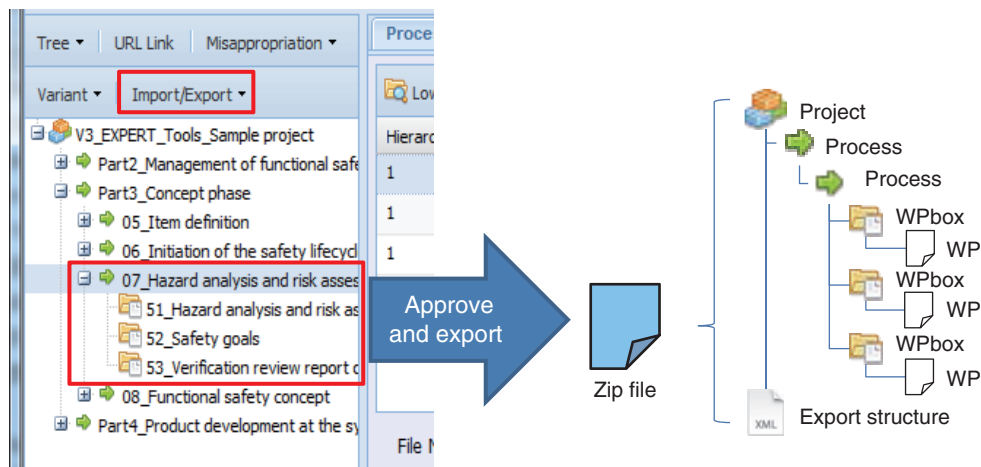


Fig. 15 Export operation

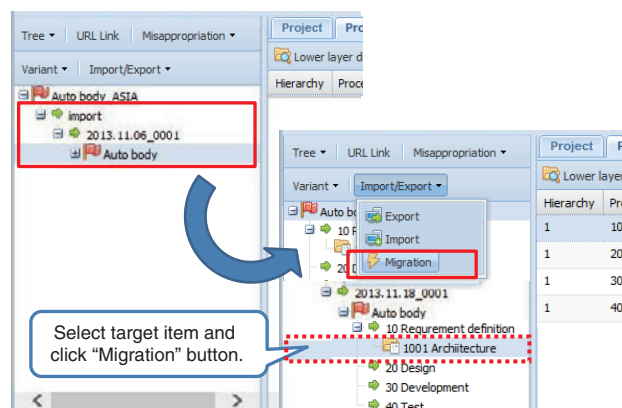


Fig. 16 Import operation

要求項目間の関連を定義することでトレーサビリティを実現した。

- (3) 開発中の検証会をイベントとしてシステムに定義し、成果物と検証結果を保存することが可能になった。
- (4) 設定された項目間の関連を一覧表示することで、影響範囲を特定できるようにし、検索工数の削減が可能になった。

参考文献

- (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

■ 著 者 ■



宅 美 仁 史



黒 崎 泰 央



石 田 宏 司