

高効率に整合された完成車全体の 機能安全プロセスの構築

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

太田 崇*
Takashi OHTA

相模 宏樹*
Hiroki SAGAMI

要 旨

ABSTRACT

ロジックを持つ電気、電子システムを自動車に搭載するためには、機能安全規格 ISO 26262 への準拠が必要である。機能安全活動は、規格に準拠したプロセスを実行することでシステムの機能不全により引き起こされる人の健康に対する身体的な被害を予防するための対策をおこなう。複数のシステムが複雑に関係する自動車開発において機能安全規格に効率良く準拠するためには、各システムの担当者が合理的に連携して完成車全体にわたる機能安全活動を実施する必要がある。そこで、完成車全体の中で個々のシステムの関係性を調査して機能安全活動境界を過不足なく設定できる手法を策定し、システムに実装されるインタフェースをガイドに各システム同士が連携して影響分析をおこない、機能安全要求を整合する独自のプロセスを機能安全プロセスに追加した。その結果、影響分析の重複範囲を削減できたことでシステム内部の影響分析の精度が向上し、システム同士を連携させるプロセスを独自に追加したことで高精度な影響分析を車両レベルで網羅的に実施して適切な機能安全要求を配置できる完成車全体の機能安全プロセスを構築できた。

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. はじめに

近年の自動車に搭載される電子制御システムの増加と複雑化に伴い、機能安全規格 ISO 26262 (Fig. 1) が制定され、2011 年 11 月に正式に発効された⁽¹⁾。一般的に車両に搭載

される電気、電子システムは、スイッチやセンサ、通信などを用いてドライバの操作状態や車両の状態を情報化して入力し、それら入力情報を用いて一つ、または複数のシステムを制御することで機能を実現しており、システム内部に機能不全が発生するとドライバ、もしくはシステムの意

*四輪 R&D センター

図通りに機構を制御できずにハザードを引き起こしてしまう (Fig. 2)。

ISO 26262 では、本質安全に加えて、人体に被害を及ぼすハザードを引き起こす電気、電子システムの故障要因を特定し、ハザードによるリスクを許容できるレベルに低減する対策が適用された開発をおこなう必要があり、車両レベルの機能を有するシステムまたはシステム群であるアイテムごとにその活動が求められている。ISO 26262 発効以前、開発活動の対象となるシステムは、主に Electronic Control Unit (ECU) や特定の機能単位で管理されていたため、システムごとにアイテムのハザード分析およびリスクアセスメント (H&R) を実施し、各システムに機能安全要求を割り当てて PART 4 システムレベルの開発 (Fig. 1) 以

降の活動を実施していた。ISO 26262 (Fig. 1) はウォータフォール型の V 字モデルの開発プロセスのため、上流工程の設計検討や分析に抜け漏れが発生した場合、手戻り工数が大きくなり、後工程で工数が増加してしまう。このことから、いかに上流工程において網羅的に整理されたアイテム境界で精度良く影響分析を実施できるかが、車両レベルで効率よく機能安全に対応するための重要なポイントになる。しかしながら、ISO 26262 においてはアイテム単位での機能安全プロセスは定義されているが、車両レベルでの複数アイテム協調開発の機能安全プロセスについては明確に定義されていない。そこで機能安全プロセスの上流工程にあたる ISO 26262 の Part 3 のコンセプト設計段階で前述の課題を解決する手段として完成車全体での適切な機能安全要求の配置を可能とする完成車全体の機能安全プロセスを構築した。

2. 開発のねらい

ISO 26262 に準拠した開発ではアイテムを機能安全活動の対象範囲とした活動が求められる。しかし、システムの担当者によってアイテム境界の決め方に差があるため、一定のルールを策定してアイテム境界を設定しなければ、完成車全体として抜け漏れによる手戻りや重複作業による無駄が発生してしまう。上流工程での影響分析の網羅性や精度が後工程の効率に影響するため、上流工程でアイテム間の連携が上手くいかない場合、他のシステムが補完的に機能安全活動をおこなっていたとしても、分析範囲の網羅

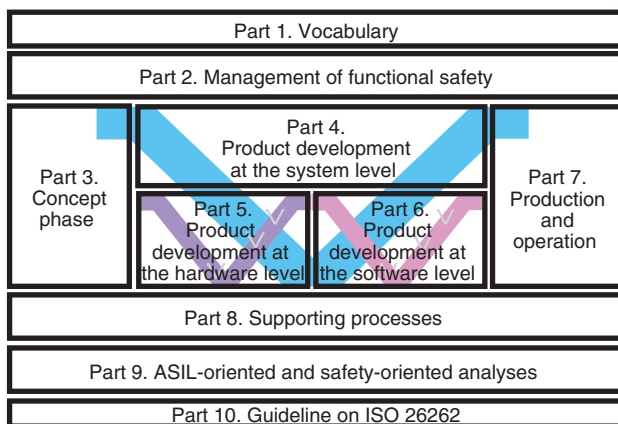


Fig. 1 Overview of ISO 26262

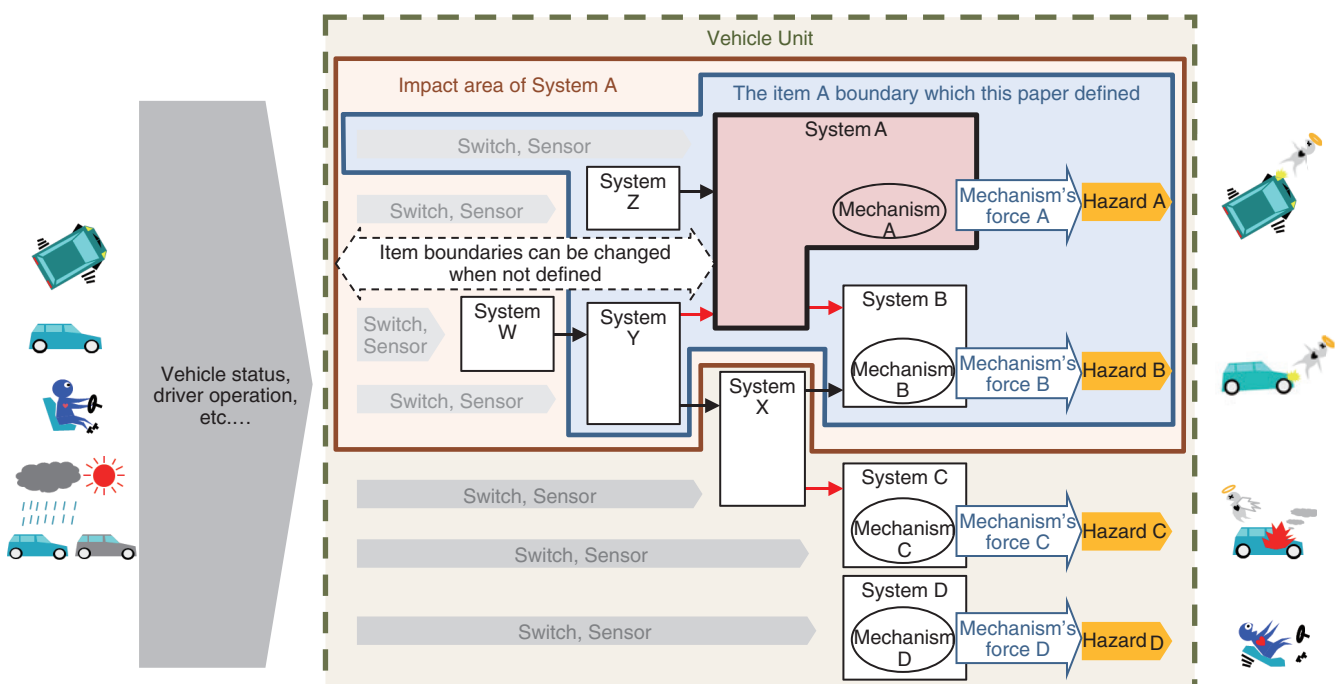


Fig. 2 Relationship among systems, item boundaries, and vehicle level

性を証明するために余計な工数が必要になる。また、個々のシステムの担当者が自分のシステムを超えた分析範囲を設定した場合、複数のシステムの担当者が重複した範囲に対して分析するため、効率的ではない。さらに、開発現場では、開発資産を再利用して差分開発をおこなうことで工数削減に取り組んでいるので、開発資産を再利用できる仕組みも必要である。

以上の観点を踏まえて、車両レベルでの高精度な機能安全活動を効率的に実施するため、本活動で構築する完成車全体の機能安全プロセスのねらいを以下に設定した。

- (1) システム間でハザードの影響や機能安全要求を伝達する経路（インタフェース）を明示する。
- (2) 不必要な影響分析範囲の重複部を最小化できるようにアイテム境界を決める仕組みをつくる。
- (3) システム間で連携したハザードの影響分析をおこない、機能安全要求を割り当てて整合できる完成車全体の機能安全プロセスをつくる。

3. 完成車全体の機能安全プロセス

以降に示すインタフェースの区分とハザードの影響伝達の仕組みをもとに、各システムが連携するプロセスを従来の機能安全プロセスに追加することで完成車全体の機能安全プロセスを構築した。

3.1. インタフェースの明示

3.1.1. インタフェースの区分

本プロセスはインタフェースをガイドとして活動することを特徴としている。そのインタフェースは、機構力、動作要求、情報の三種類に区分される。機構力は、物理的な影響を伝達するインタフェースであり、動作要求は、他のシステムの機構力を操作するインタフェースである。また、情報は、ハザードに直接影響を与えるかどうか不明なインタフェースである。

3.1.2. ハザードの影響伝達の仕組み

ハザードの影響が伝達する仕組みの例を、システムを四角、機構を楕円、情報を黒の矢印、動作要求を赤の矢印、機構力を群青色の矢印、ハザードを橙色の矢印で表し、Fig. 3(a) から (d) に示す。例えば、システム E の内部故障によりシステム E が機構を誤って制御して異常な機構力を発生させることでハザードが発生する [Fig. 3(a)]。機構を持たないシステム F であっても、システム G に対して動作要求を出力した場合、システム G の機構に影響を与えハザードを発生させる [Fig. 3(b)]。また、ハザードの影響は、ハザードの発生要因となる機構を持つシステム J から、情報およびシステム I やシステム H を通じてスイッチやセンサなど車両レベルの入力まで伝達される [Fig. 3(c)]。このようなハザードの影響を軽減するために、ハザードと車両

レベルの入力との間に配置されるシステムに安全機構を実装することなども考えられる [Fig. 3(d)]。

以上のインタフェースの区分とハザードの影響伝達の仕組みをもとにシステム間のインタフェースを明示した標準

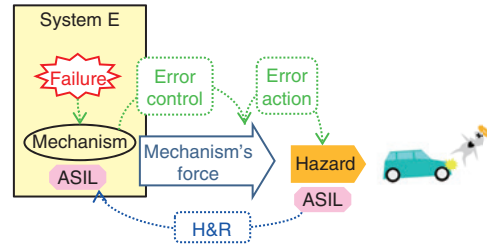


Fig. 3(a) Hazard occurrence

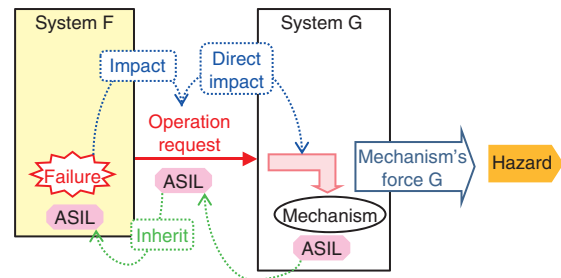


Fig. 3(b) Hazard due to operation request

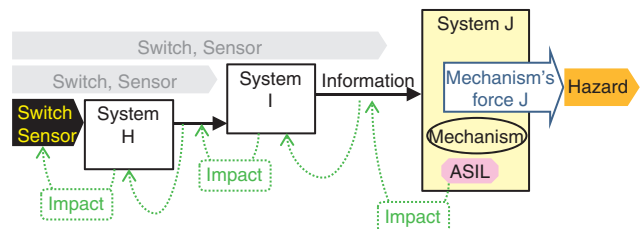


Fig. 3(c) Transmission path of hazard impact

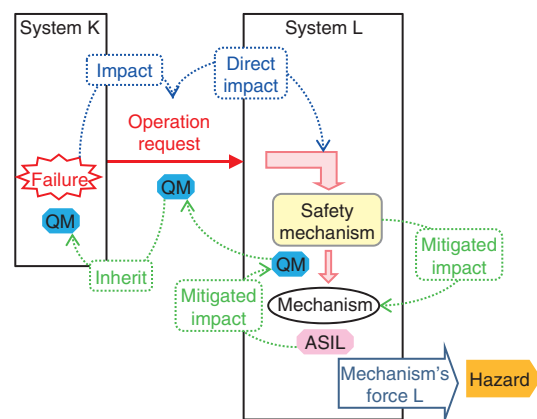


Fig. 3(d) Mitigation of hazard impact by safety mechanism

アーキテクチャ (Fig. 5) を作成した。この標準アーキテクチャを用いてインタフェースをガイドにシステムの担当者同士が連携して影響分析をおこない、機能安全要求を整合するプロセスを構築したことで、システムの担当者は、どこから、どれくらいの、どんなリスクが自システムに存在するかがわかりやすくなり、適切な機能安全要求の割り当てが容易になった。

3.2. 影響分析範囲の重複部の削減

3.2.1. アイテム境界条件

3.1.2. 項に示したようにシステムは、機構力や動作要求を出力して直接的にハザードを引き起こし、情報を介して間接的にハザードを引き起こすと考えられる。このため、隣接するシステム間で適切な機能安全要求を割り付けられれば、ハザード要因となる経路全てで安全方策を実施することができるので、以下のようにアイテム境界条件を設定した。

インタフェースを入力した場合は、インタフェースを通じて連結されたシステムと機構をアイテム範囲に取り込む。また、インタフェースを出力した場合は、インタフェースを通じて連結されたシステムと機構、機構力、関連ハザードをアイテム範囲に取り込む。

3.2.2. 前提条件

プロセスの前提条件は以下である。インタフェースを介して伝達されるハザードの影響の大きさを ASIL で示す。また、システムごとに担当者が配置され、機能安全要求を割り当てられたシステムの担当者は、PART 4 システムレベルの開発 (Fig. 1) 以降の活動で安全方策を実施する。

以上のアイテム境界条件と前提条件をもとに完成車全体でアイテム境界を整理して標準アーキテクチャを作成した。この標準アーキテクチャを用いてシステムの担当者同士が連携して影響分析をおこなうプロセスを構築したことで不必要な影響分析の重複範囲を削減できたので、システムの担当者は、自システム内を集中的に影響分析できるようになった。

3.3. 完成車全体の機能安全プロセス

システムの担当者とプロセス管理者が協力して以下のプロセス (1) から (6) を実施する。システムの担当者は、自システムのアイテムを機能安全活動の対象範囲としてプロセス (2) から (4)、プロセス (6) を実施する。また、プロセス管理者は、各システムの進捗を管理し、完成車全体の機能安全活動を実施する (Fig. 4)。

プロセス (1) プロセス管理者による開発車両のアイテムごとの基礎アーキテクチャ作成と配布

プロセス (2) システムの担当者による初期アーキテクチャの作成

プロセス (3) システムの担当者によるハザードの影響分析

プロセス (4) システムの担当者間での機能安全要求の整合

プロセス (5) プロセス管理者による標準アーキテクチャの更新

プロセス (6) システムの担当者による PART 4 システムレベルの開発 (Fig. 1) 以降の機能安全活動

上記のプロセス (1) から (6) の詳細を以下に説明する。

3.3.1. プロセス管理者による開発車両のアイテムごとの基礎アーキテクチャ作成と配布

標準アーキテクチャの作成においてプロセス管理者は、車両に搭載されるシステムと関連システムの関係性を調査して 3.2.1. 項に示したアイテム境界条件を適用し、標準アーキテクチャを作成する (Fig. 5)。基礎アーキテクチャの作成と配布では、車両開発が開始された時、プロセス管理者は、開発車両に搭載されるシステムを確認し、標準アーキテクチャから必要なシステムに限定した基礎アーキテクチャを作成し、各システムの担当者に配布する (Fig. 6)。

3.3.2. システムの担当者による初期アーキテクチャの作成

開発車両で使用するインタフェースの特定では、システムの担当者は、基礎アーキテクチャをもとに関連システムの担当者とのインタフェースの使用、不使用の整合をおこない自システムの初期アーキテクチャを作成する (Fig. 7)。初期アーキテクチャを作成する際にインタフェースや関連システムが足りない場合、システムの担当者は、関連システムの担当者と整合して、プロセス管理者に初期アーキテクチャの変更を要求する。

プロセス管理者は、変更対象のシステムの初期アーキテクチャを更新する。

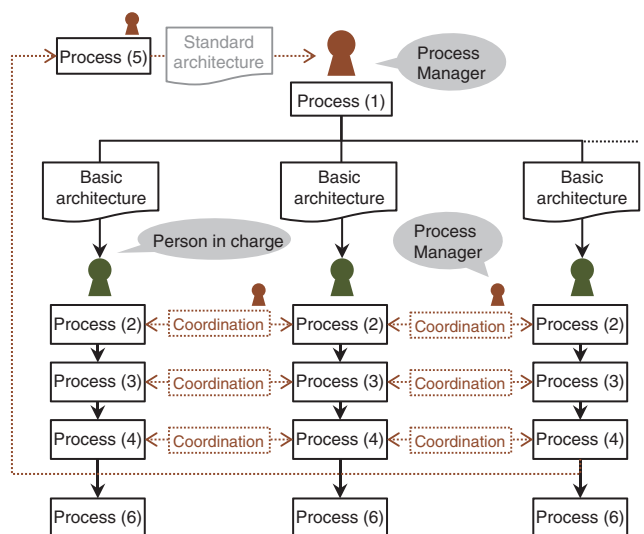


Fig. 4 Functional safety processes at vehicle level

3.3.3. システムの担当者によるハザードの影響分析

機構力のハザードレベルの分析では、自システムが出力として機構力を持つ場合、システムの担当者は、H&Rを実施して機構力が持つハザードのASIL を評価する。

自システムが、ASIL 対象の機構力に作用する動作要求を入力している場合、入力する動作要求に ASIL を割り当て、動作要求を出力するシステムの担当者に通知する。動作要求を出力するシステムの担当者は、通知された ASIL

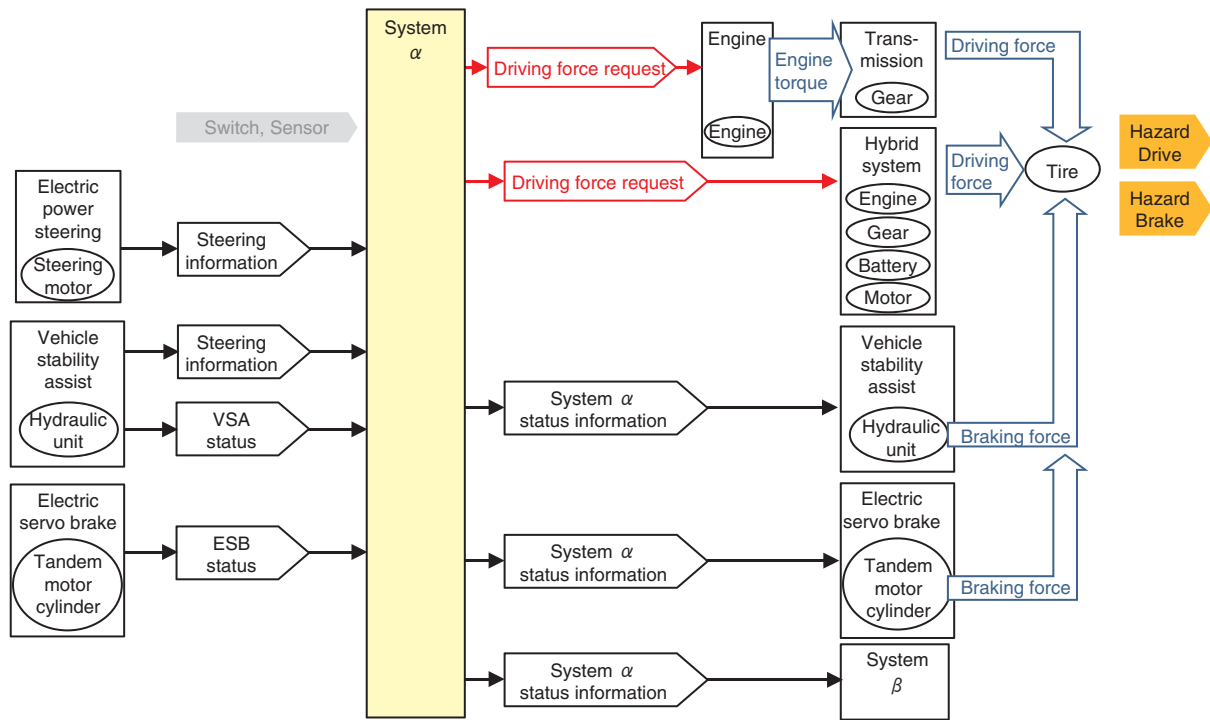


Fig. 5 Standard architecture

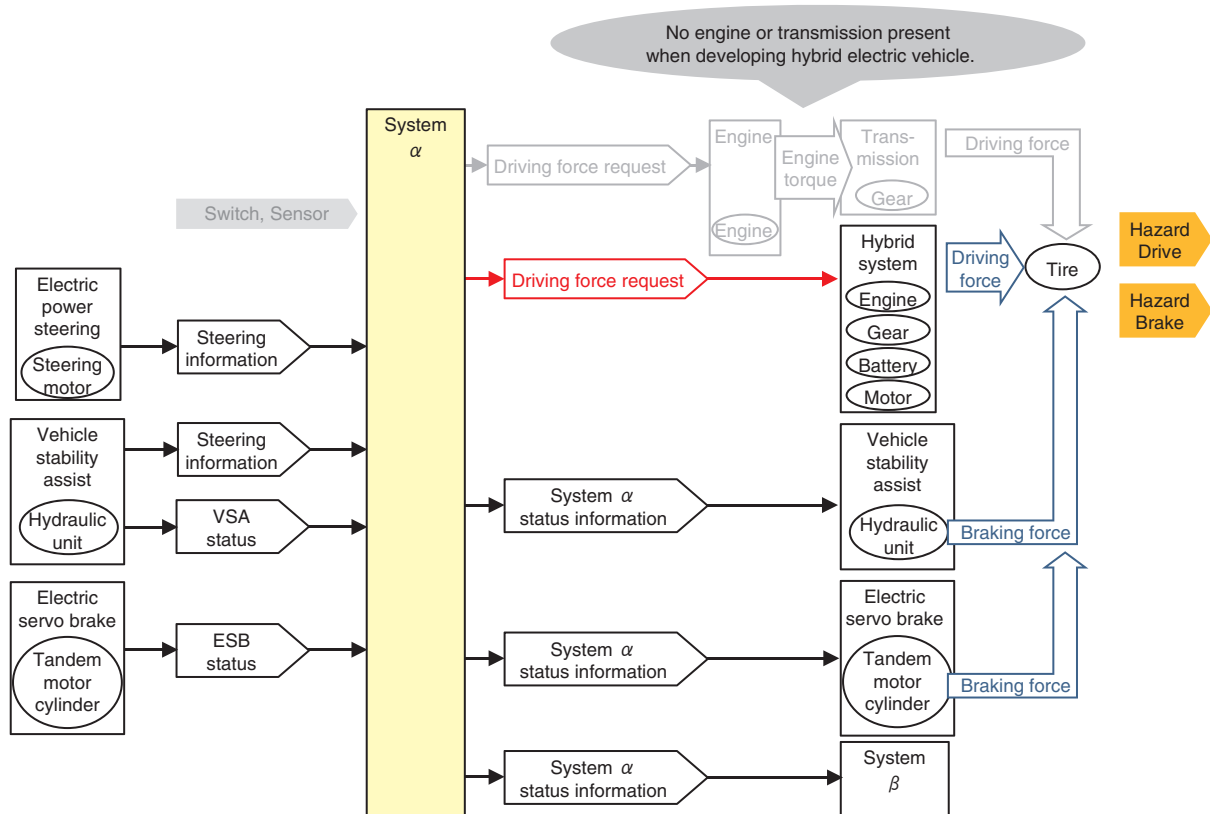


Fig. 6 Basic architecture

を確認し、出力する動作要求に通知されたASIL を割り当てる (Fig. 8).

安全機構を想定したコンセプト設計と影響分析では、システムの担当者は、安全機構要素の配置を想定した自シ

テムのコンセプト設計をおこない、システム内部の影響分析を実施して自システムに実装されたインタフェースにASIL を割り当て、関連システムの担当者に通知する (Fig. 9). 割り当てられたASIL の確認では、自システムのイン

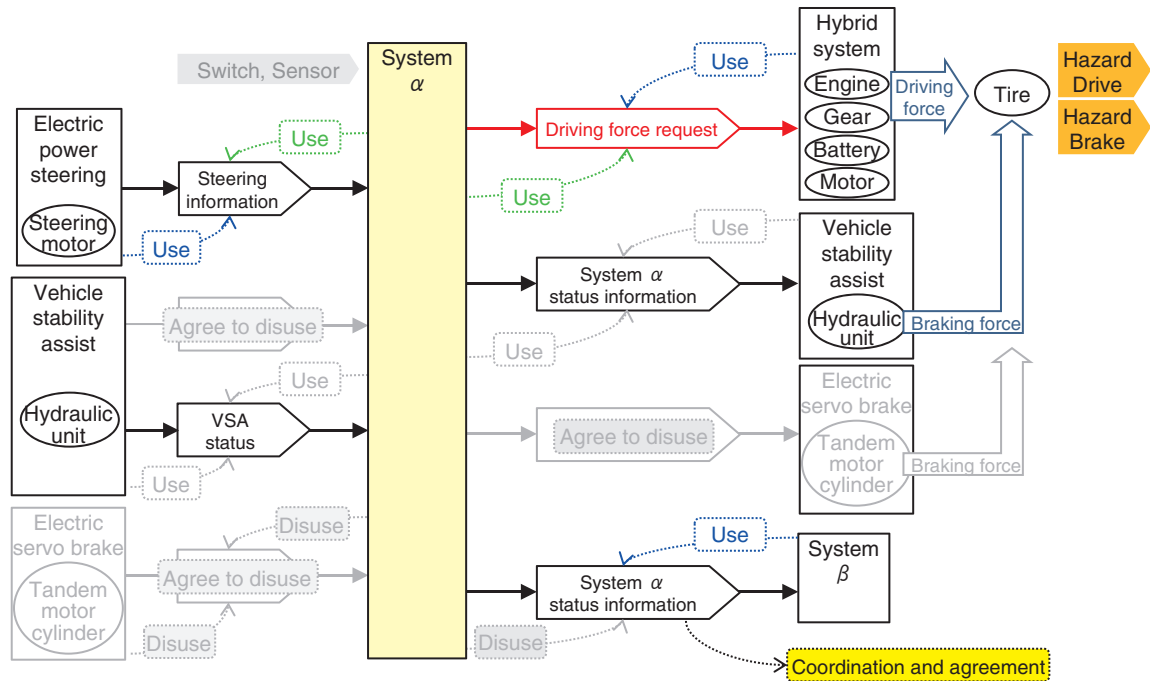


Fig. 7 Process of creating preliminary architecture

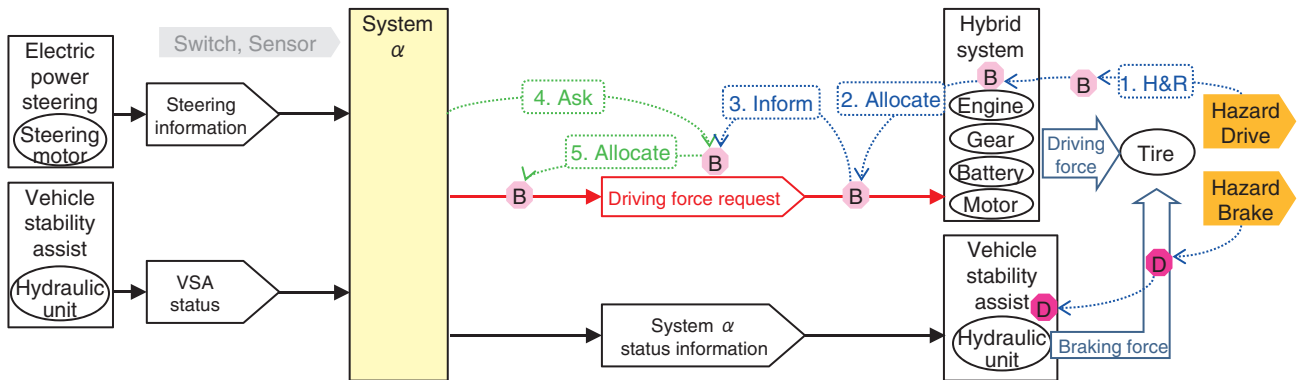


Fig. 8 Hazard analysis and risk assessment of mechanism's force and impact analysis of operation request

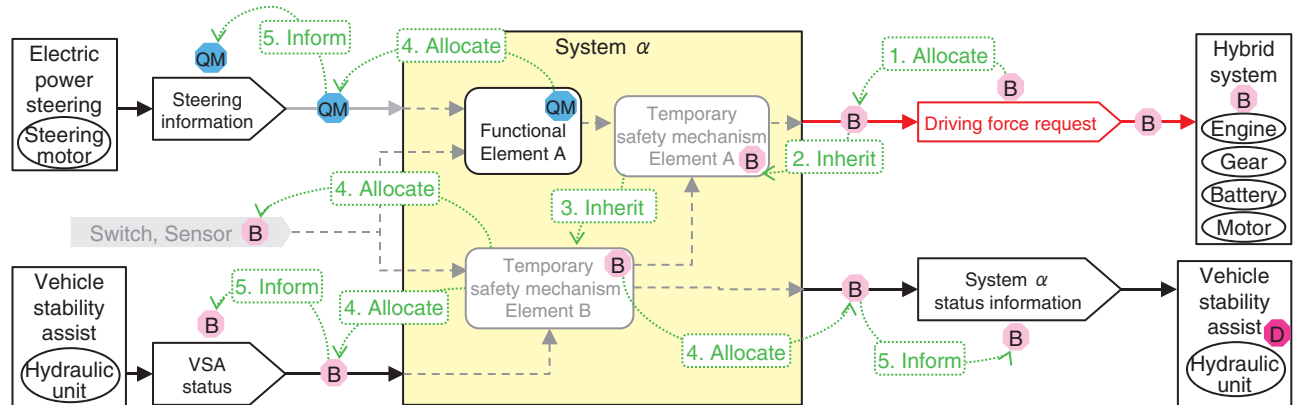


Fig. 9 Concept design assuming allocation of safety mechanisms, and impact analysis between systems

タフェースに割り当てられたASILを確認してコンセプト設計で想定した安全機構の有効性を確認し、例えば、想定したASILよりも高いASILが割り当てられた等の場合は、コンセプト設計と影響分析を再度実施する (Fig. 10)。

3.3.4. システムの担当者間での機能安全要求の整合

自システムの機能安全要求の割り当てと整合では、自システムにてASILを割り当てたインタフェースに対する安

全機構を関連システム側に実装してもらう場合、そのインタフェースに機能安全要求を割り当て、関連システムの担当者と機能安全要求の内容を合意する (Fig. 11)。関連システムに割り当てられた機能安全要求の確認と整合では、自システムのインタフェースに関連システムから機能安全要求を割り当てられた場合、関連システムの担当者と機能安全要求の内容を合意する (Fig. 12)。

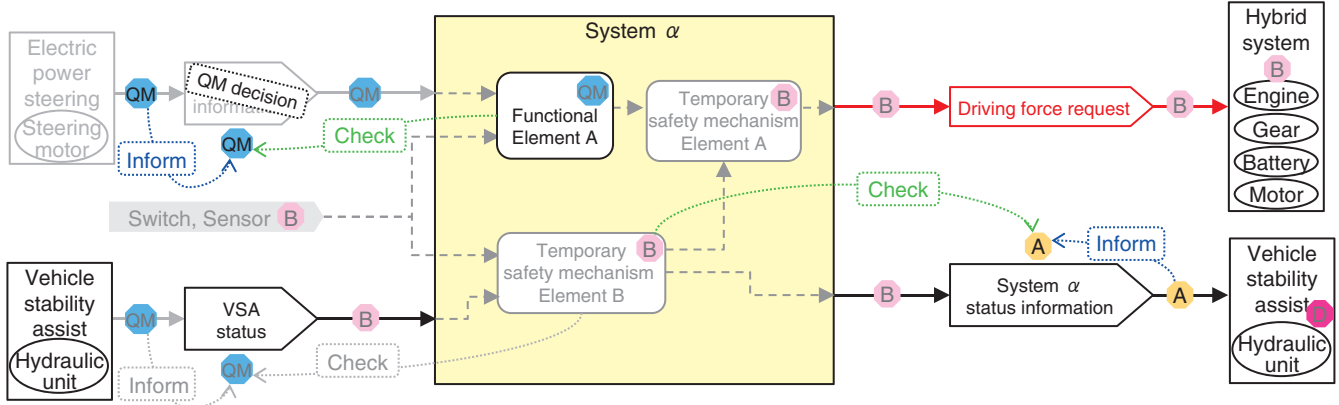


Fig. 10 Check for allocated ASILs

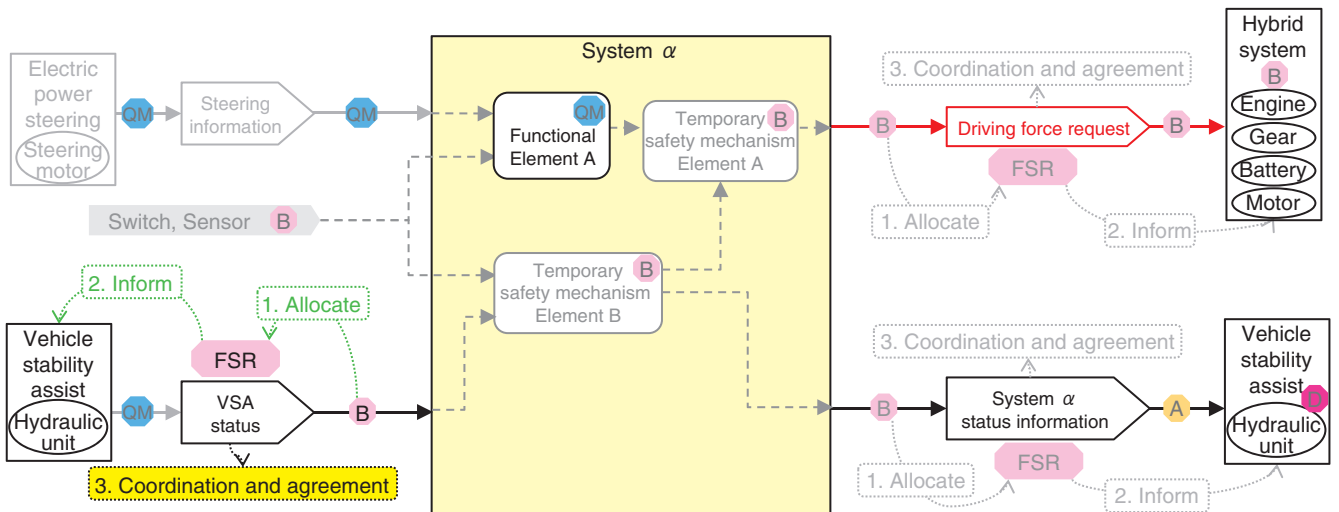


Fig. 11 Coordination and agreement of functional safety requirements assigned to other systems

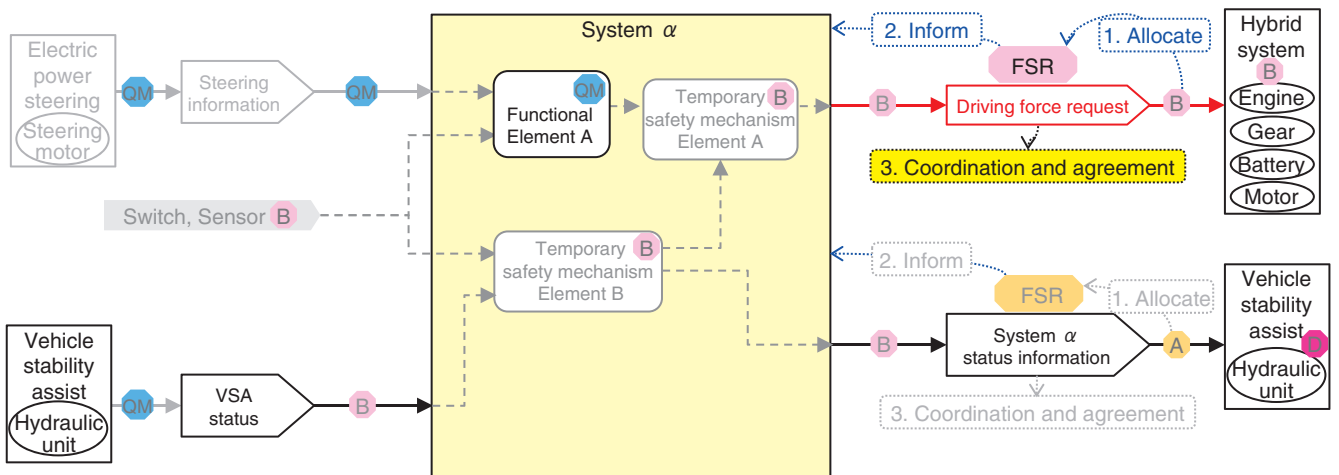


Fig. 12 Coordination and agreement of functional safety requirements assigned from other systems

3.3.5. プロセス管理者による標準アーキテクチャの更新
完成されたアーキテクチャにインタフェースが新たに追加されていた場合、プロセス管理者は、追加されたインタフェースを標準アーキテクチャに追加する。

更新された標準アーキテクチャは、次の車両開発時に開発資産として使用される。

3.3.6. システムの担当者による PART 4 以降の機能安全活動

3.3.1. 項から 3.3.5. 項の活動で自システムに割り当てられた機能安全要求を、自システム内でもともと割り当てられている機能安全要求に追加して PART 4 以降の機能安全活動を実施する⁽²⁾。

以上のように完成車全体の中でアイテム境界を整理し、システム間のインタフェースを明示した標準アーキテクチャを用いてシステムの担当者が連携して実行する完成車全体の機能安全プロセスを構築したことで、車両レベルでの機能安全活動において機能安全要求の割り当ての抜け漏れの確認が容易になった。また、機能安全要求の整合を終えた段階の完成度の高い標準アーキテクチャを次の車両開発時に再利用する工程をプロセスに組み込んだことで差分開発が容易になり、効率的な完成車全体の機能安全プロセスを構築できた。

4. まとめ

本プロセスを構築することにより、以下を得ることができた。

- (1) 機構力、動作要求、情報の三種類にシステム間のインタフェースを区分してシステム間の関係性を明示できたので、システムの担当者は、どこから、どれくらいの、どんなリスクが自システムに存在するかがわかりやすくなり、適切な機能安全要求の割り当てが容易になった。
- (2) インタフェースを通じて連結されたシステムと機構、機構力、関連ハザードをアイテム範囲に取り込むアイテム境界条件を設定したことで、不必要な影響分析の重複範囲を削減できたので、システムの担当者は、自システム内を集中的に影響分析できるようになった。
- (3) プロセス管理者が各システムの進捗管理をした上で、システムの担当者同士が連携して影響分析を実施し、機能安全要求を整合する完成車全体の機能安全プロセスができたので、機能安全要求の割り当ての抜け漏れの確認が容易になった。

参考文献

- (1) ISO 26262: Road Vehicles-Functional Safety, (2011)
- (2) 相模宏樹, 広中慎司, 森良司, 向井拓幸: モデルベース

設計を用いた ISO 26262 対応システム設計プロセス,
Honda R&D Technical Review, Vol.26, No.2, p.165-171

APPENDIX

本稿中で使用した用語の説明を機能安全規格 ISO 26262 から抜粋し、以下に示す。

(1) アイテム

車両レベルの機能を実装するシステムまたはシステム群

(2) ハザード

アイテムの機能不全の振る舞いにより引き起こされる人の健康に対する身体的な障害または被害になりうる原因

(3) ASIL

自動車用安全水準 (Automotive Safety Integrity Level). A, B, C, D があり, ASIL A が最も低い安全度水準で ASIL D が最も高い安全度水準を持つ。

(4) QM

ASIL A 未満の安全度水準で ISO 26262 の要件管理下に置かれず、通常の品質管理で管理される。

■ 著 者 ■



太田 崇



相模 宏樹