STAMP/STPAの自動車向け活用ガイド
～JASPAR機能安全WG活動成果紹介～

2017.11.28

Japan
Automotive
Software
Platform
and
Architecture

JASPAR　機能安全WG

技術アドバイザ　宮崎　義弘（日立オートモティブシステムズ㈱）
主査　岡田　学　（日産自動車㈱）

一般社団法人JASPAR

目次

(1) JASPAR機能安全WGの全体活動

(2) STAMP/STPAの自動車向け活用ガイドの概要

(3) 自動車用機能安全規格ISO 26262との差分分析

(4) 対象システム事例（仮想 EPBシステム）

(5) 分析事例

(6) 提唱

(7) まとめ

EPB: Electric Parking Brake

(1) JASPAR機能安全WGの全体活動

(2) STAMP/STPAの自動車向け活用ガイドの概要

(3) 自動車用機能安全規格ISO 26262との差分分析

(4) 対象システム事例 (仮想 EPBシステム)

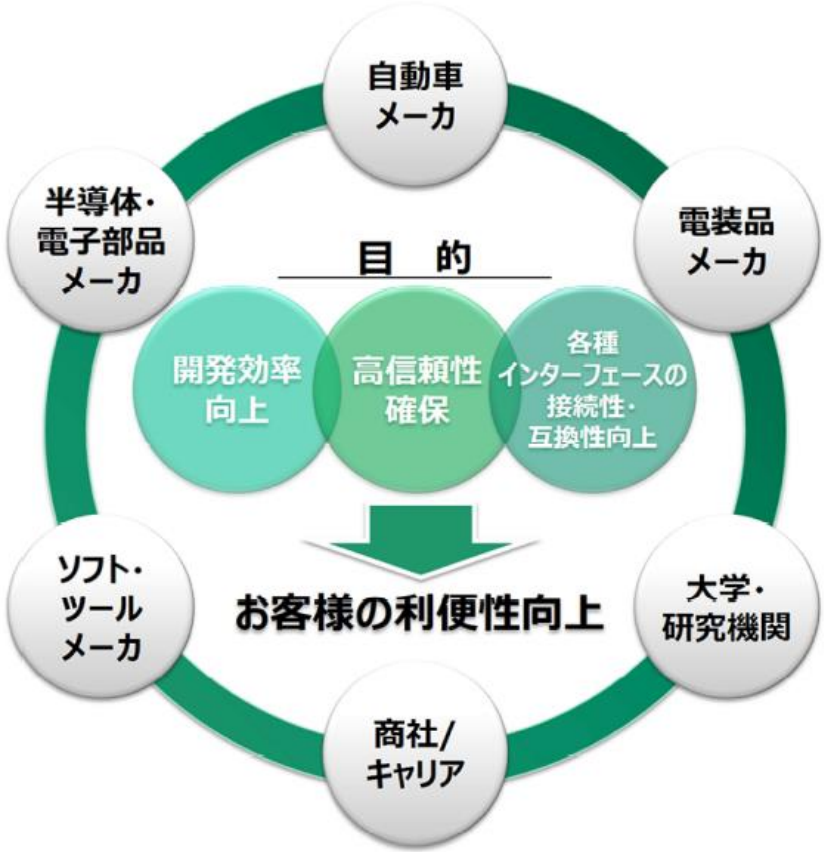
(5) 分析事例

(6) 提唱

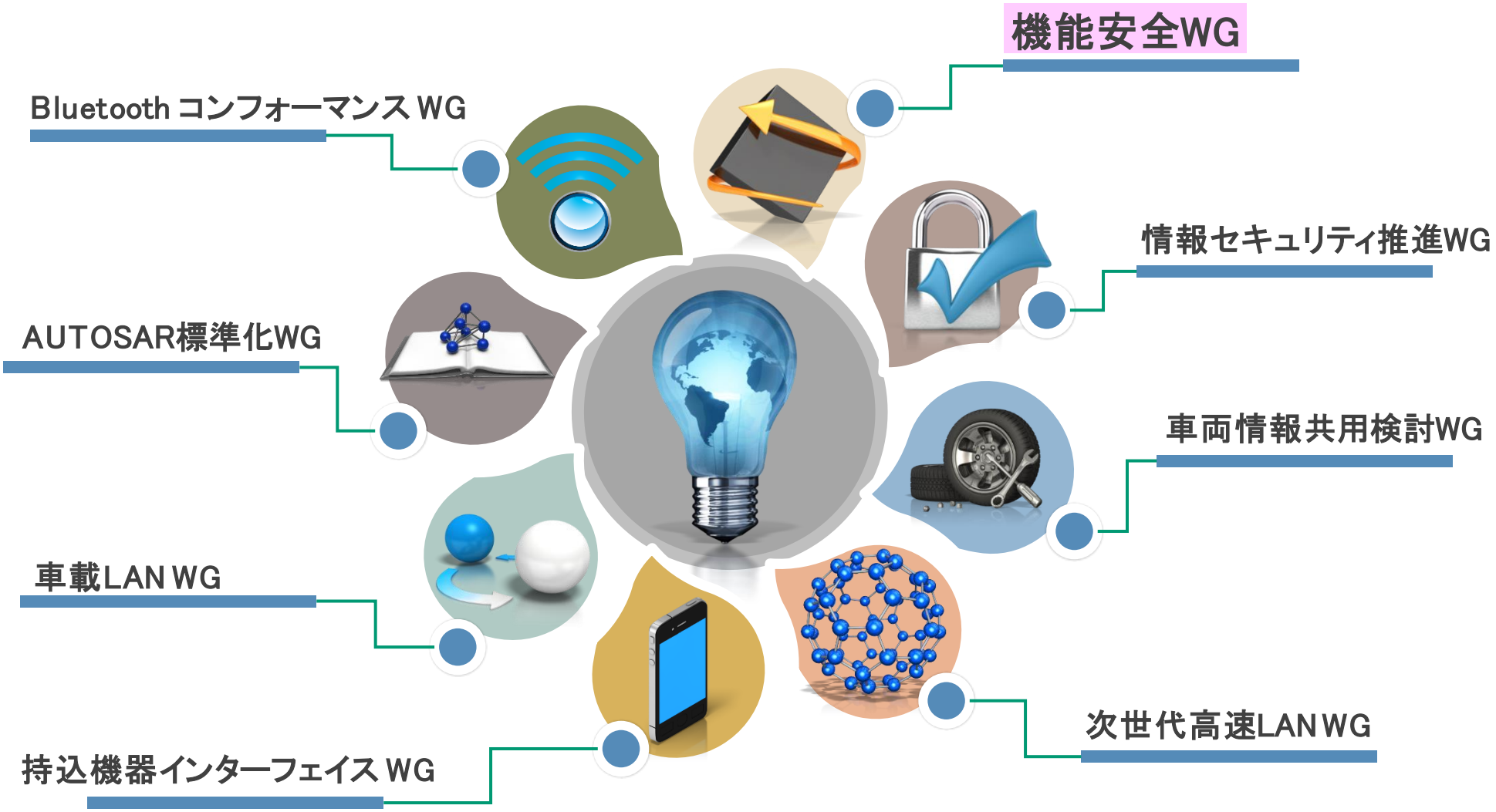
(7) まとめ

JASPARについて

◆団体名： 一般社団法人JASPAR（Japan Automotive Software Platform and Architecture）
◆設立： 2004年　　◆会員数： 166社（2017年4月）
◆設立背景： 高度化・複雑化する車載電子制御システムのソフトウエアやネットワークの標準化及び共通利用による、開発の効率化と高信頼性確保を目指す。
◆活動概要：
自動車メーカ、電装品メーカ、半導体・電子部品メーカ、ソフト・ツールメーカ、商社/キャリアの各業種、大学・研究機関から技術者が参画し、海外・国内の関連団体との協調の下、車載ネットワーク、ソフトウエア、情報セキュリティにおける標準化を推進する。
◆ミッション：
自動車の進化に伴うカーエレクトロニクス領域での将来の共通課題を特定し、その解決のための標準化活動に取り組み、自動車産業全体の公正な競争基盤の創造・開発の生産性向上と技術発展を促進する。
◆公開HP： https://www.jaspar.jp/

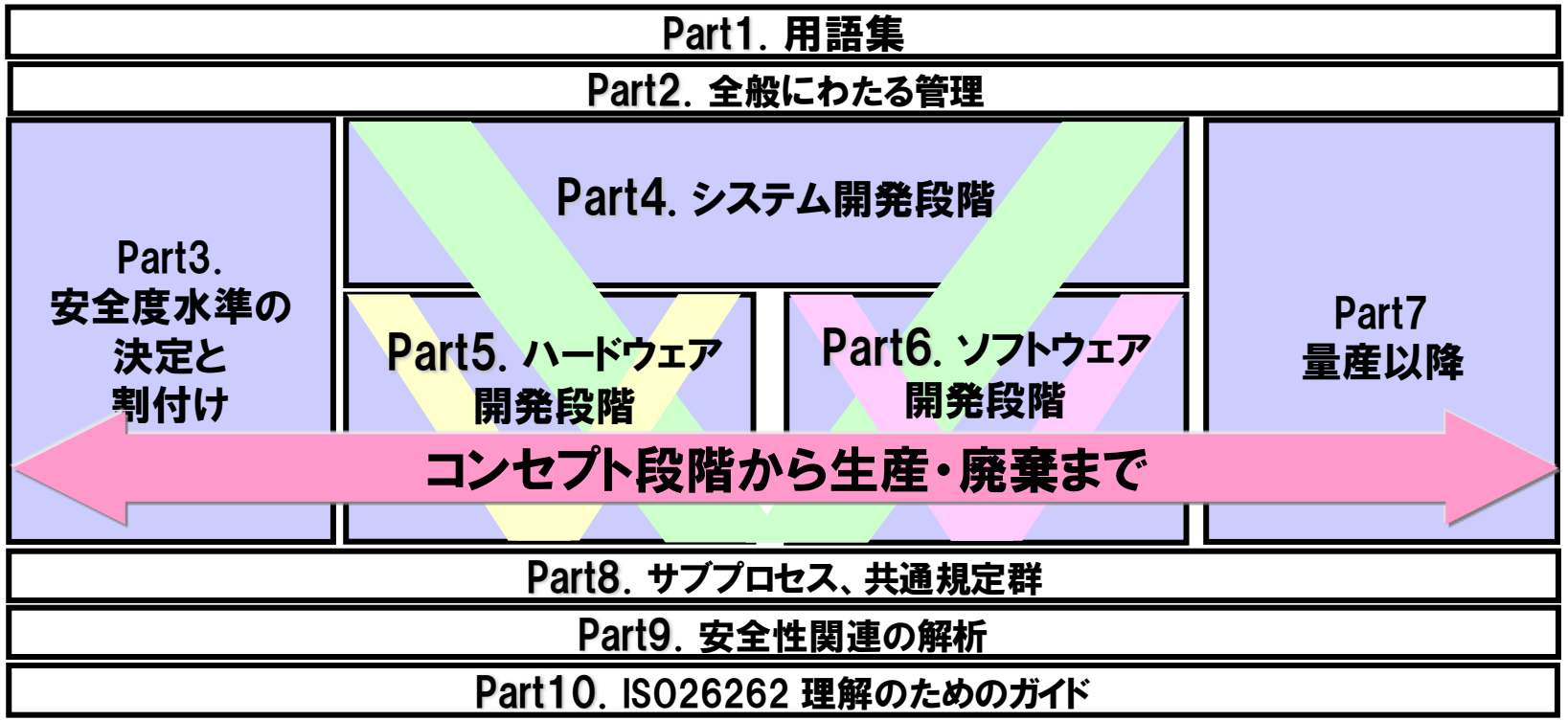


JASPARのワーキンググループ



自動車用機能安全規格 ISO 26262

◆自動車用機能安全規格ISO 26262として2011年11月に発効
◆開発初期から廃棄に至る自動車の全ライフサイクルをカバーした構成
◆機能安全の視点で、設計・検証したことを示すよう要求
　1）ハザード解析、リスク評価を実施し、目標安全度水準（ASIL）を設定
　2）目標安全度水準（ASIL）を達成するような安全機能のモノづくり
　3）目標が達成されていることを証明



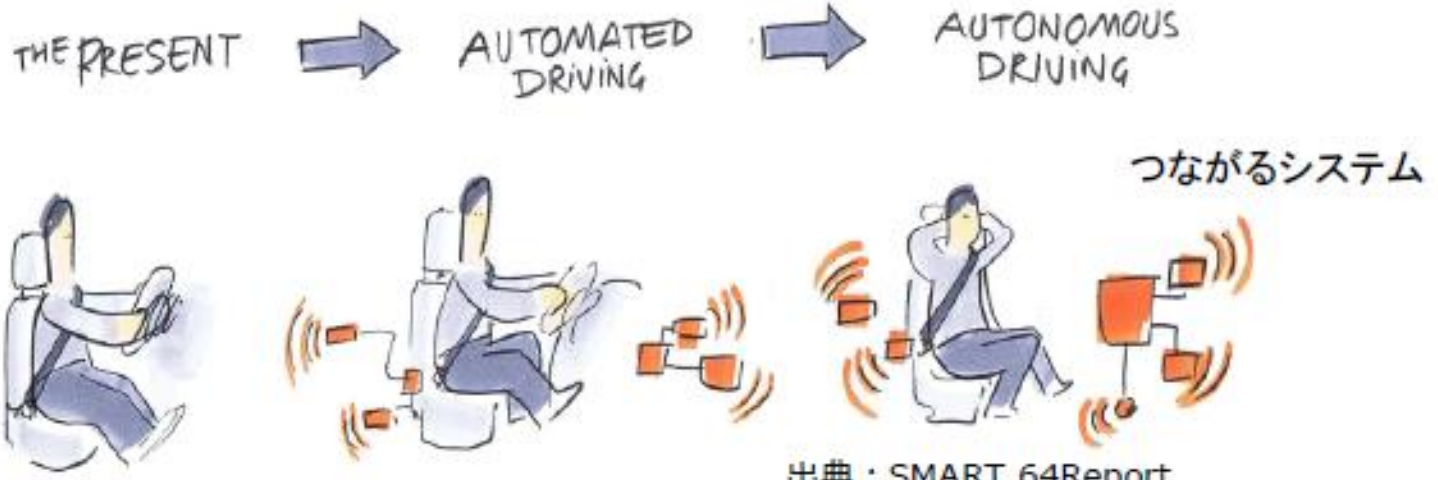
ISO 26262（Ed1）の構成

機能安全に関わる環境変化と取組み

2011年
ISO 26262: 1st Edition発効
単機能システムが中心

2017年～
自動運転など
超大規模システムへの対応

機能の進化

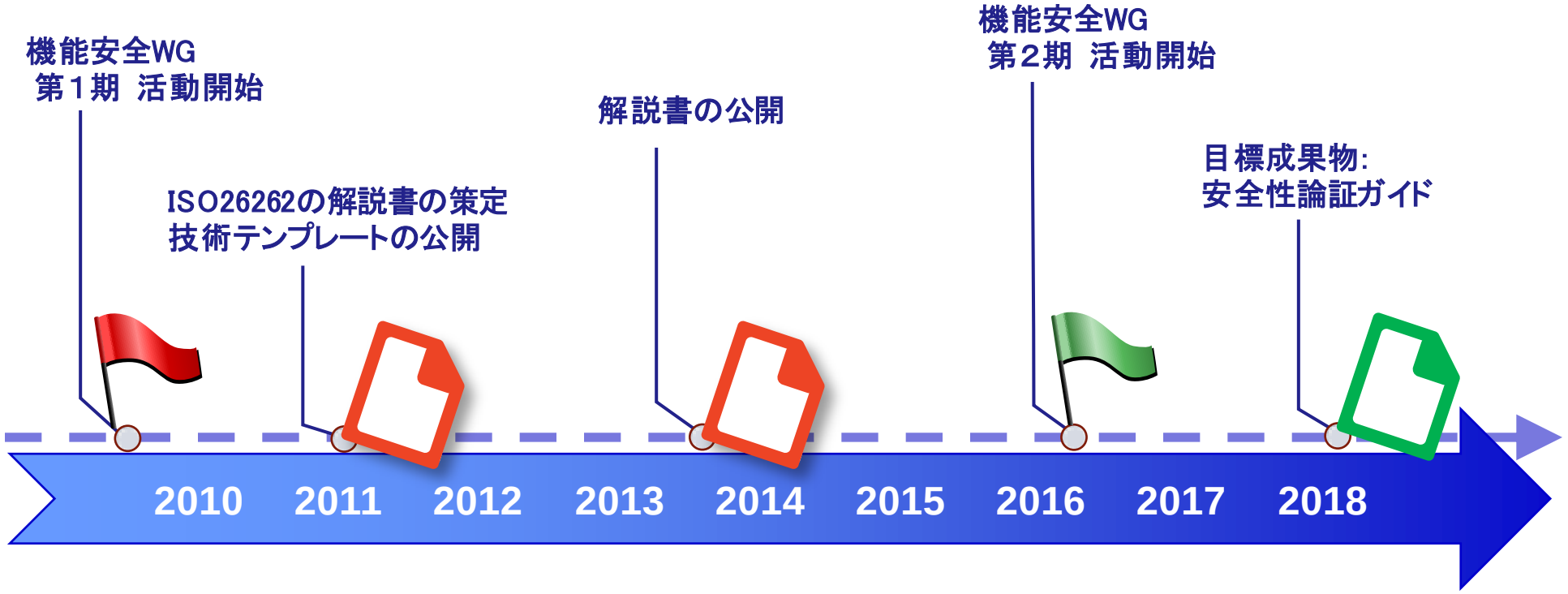


出典：SMART 64Report

進化に対応できる取組みへ

技術テンプレート、解説書 ➡ より広い視点での対応要！

JASPAR 機能安全WGの活動経緯



◆機能安全WG 第２期（１６年度～）の活動目標

【目的】　機能安全設計における**安全性論証を効果的･効率的**にする

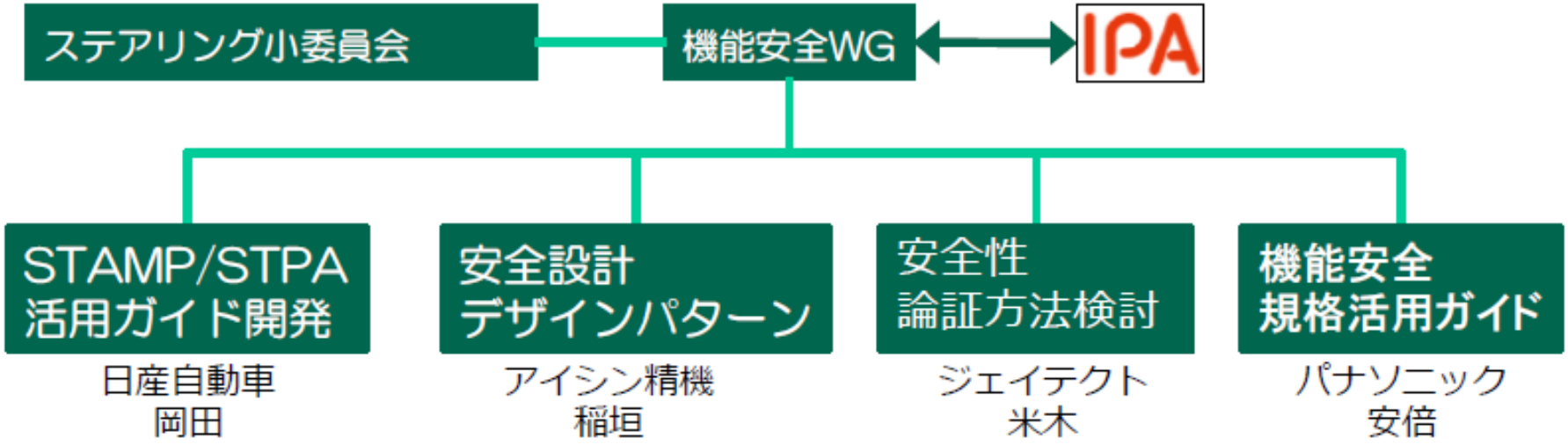
【目標成果物】　**安全性論証ガイド**

例）
- STAMP/STPA活用
- 安全設計デザインパターン
- モデル適用
- ソフトウェアパーティショニング　etc.

課題点に対する
技術の深堀

JASPAR 機能安全WGの体制(17年度)

主査：日産自動車 岡田
副主査：アドヴィックス 河野
技術アドバイザ：日立オートモティブシステムズ 宮崎
運営アドバイザ：日産自動車 大村
書記局：OTSL 山本、曙ブレーキ工業 堀



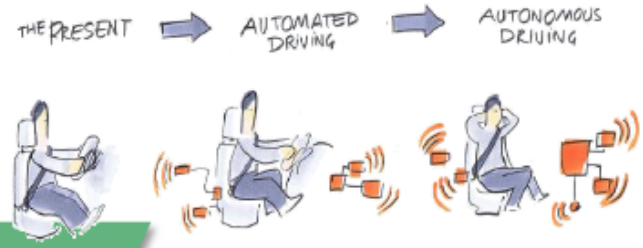
WG参加企業(17年度)

４１社　（※50音順、敬称略、2017年11月）

アイシン･エイ･ダブリュ(株)、アイシン精機(株)、曙ブレーキ工業(株)、(株)アドヴィックス、アルプス電気(株) 、イータス㈱ 、(株)ヴィッツ、SCSK(株) 、(株)OTSL 、オートリブ㈱ 、オートリブ日信ブレーキシステムジャパン(株) 、㈱オーバス、オムロンオートモーティブエレクトロニクス(株) 、カルソニックカンセイ(株) 、キャッツ(株) 、(株)ジェイテクト、ジヤトコ㈱ 、スズキ(株)、スタビリティ(株)、住友電装(株) (住友電工Gr) 、㈱チェンジビジョン、㈱デンソー、 (株)デンソーテン 、(株)東海理化、東芝デバイス&ストレージ(株)、東芝情報システム(株) 、トヨタ自動車(株) 、(株)豊田自動織機、日産自動車㈱ 、日本アイ・ビー・エム㈱ 、日本精工(株) 、日本電産エレシス(株) 、パナソニック(株) 、日立オートモティブシステムズ(株) 、(株)日立産業制御ソリューションズ、㈱富士通ビー・エス・シー、ベクター･ジャパン(株) 、ボッシュ(株) 、(株)本田技術研究所、三菱電機(株) 、矢崎総業(株)

JASPAR 機能安全WGの取組み(１７年度)

■ 自動車機能の進化における課題



OEM

安全分析
設計

Tier1

安全分析
設計

TierN

詳細設計

1．人-システム-環境 間の連携不備
2．複雑系システム間の干渉問題

STAMP/STPA
活用ガイド開発

エキスパートナレッジの共有による設計
・要求の変化を予め想定し納期短縮
・設計のパターン化による互換性向上

安全設計
デザインパターン

異なる組織間の連携方法は？
・手法/プロセスの業界共通認識
・説明の構造化と可視化

機能安全
規格活用ガイド

安全性
論証方法検討

OEM－TierN間の共創を促す環境づくり

(1) JASPAR機能安全WGの全体活動

(2) STAMP/STPAの自動車向け活用ガイドの概要

(3) 自動車用機能安全規格ISO 26262との差分分析

(4) 対象システム事例 (仮想 EPBシステム)

(5) 分析事例

(6) 提唱

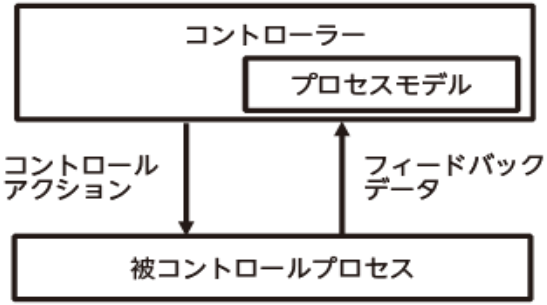
(7) まとめ

STAMP/STPAの概要

マサチューセッツ工科大学(MIT)のNancy G Leveson教授によって提唱されたシステム安全分析手法

◆STAMP（Systems Theoretic Accident Model and Processes）：
システム理論に基づくアクシデントモデル

システムの安全性は構成要素の相互作用から創発される。
システムのアクシデントの多くは、システム構成要素の故障によって起きるのではなく、システムの中で安全のための制御を行う要素（コントローラ：Controller）と制御される要素（被コントロールプロセス：Controlled Process）の相互作用が働かないことによって起きる

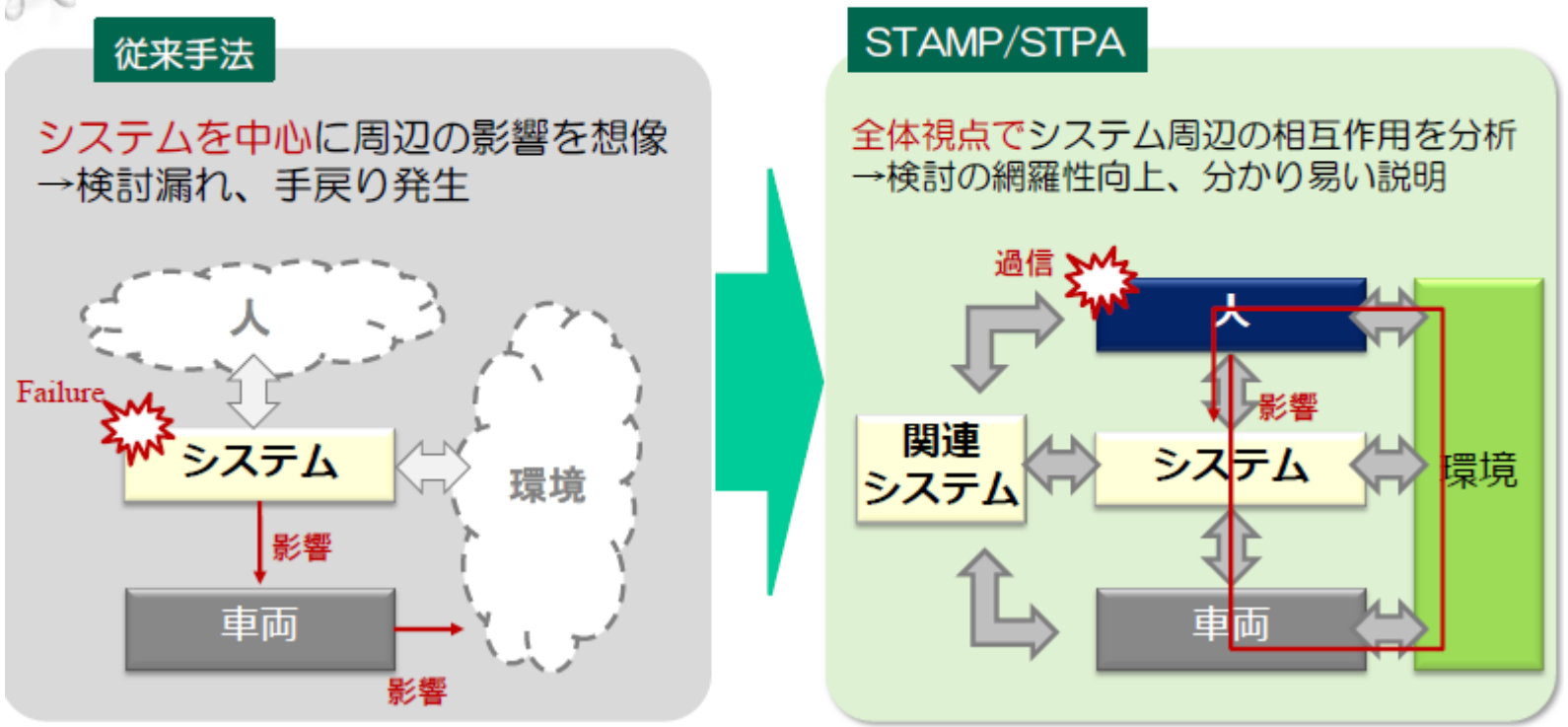


◆ STPA（System Theoretic Process Analysis）：
STAMP アクシデントモデルを前提として、システムのハザード要因を分析する安全解析手法

STPA の手順の概要
Step 0：（準備1）アクシデント、ハザード、安全制約の識別
Step 0：（準備2）コントロールストラクチャの構築
Step 1：非安全なコントロールアクション（UCA）の抽出
（「与えられない」、「与えられる」、「早すぎ、遅すぎ、誤順序」、など）
Step 2：ハザード要因（HCF）の特定
（「コントロール入力や外部情報の誤りや喪失」、「不適切なフィードバック、あるいはフィードバックの喪失」など）

出典： はじめてのSTAMP/STPA　IPA発行　http://www.ipa.go.jp/sec/reports/20160428.html

- 高機能化/複雑化する分析対象の安全分析を補強
  - 総合的な視点へ
  - 安全分析範囲の拡張
  - 検討過程の可視化による論証性向上



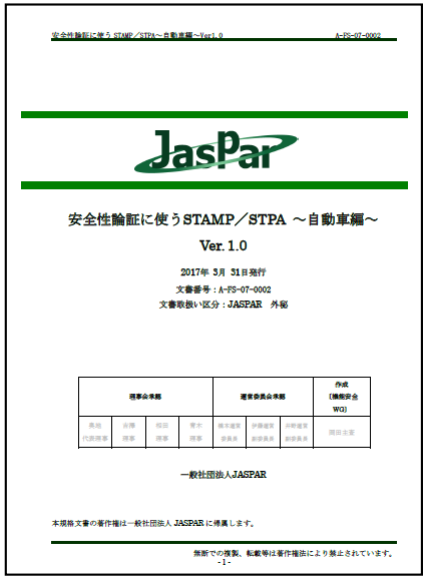
◆参加メンバ（１７年度）　１７社　（※50音順、敬称略、2017年１１月）

アイシン･エイ･ダブリュ(株)、(株)アドヴィックス、(株)ヴィッツ、(株)OTSL、オムロンオートモーティブエレクトロニクス(株) 、独立行政法人 情報処理推進機構(IPA)、スズキ(株)、㈱チェンジビジョン、(株)デンソーテン、東芝デバイス＆ストレージ(株)、トヨタ自動車(株)、日産自動車㈱ 、日本精工(株)、日立オートモティブシステムズ(株) 、(株)日立産業制御ソリューションズ、(株)本田技術研究所、三菱電機(株)

STAMP/STPA活用ガイド開発チームの活動風景

活動成果物「STAMP/STPA活用ガイド」の概要

ガイド名称: **安全性論証に使うSTAMP／STPA ～自動車編～**


安全性論証に使うSTAMP／STPA ～自動車編～
Ver. 1.0
2017年 3月 31日発行
文書番号：A-PS-07-0002
文書取扱い区分：JASPAR 外秘
一般社団法人JASPAR
本規格文書の著作権は一般社団法人 JASPAR に帰属します。

目次:

1. はじめに
2. 概要
3. 本書で取り扱う事例説明
4. STAMP/STPA EPB事例説明
5. 安全性論証に使うSTAMP/STPA EPB事例説明
6. Q&A
7. おわりに

付録:各社EPB分析事例

自動車用機能安全規格ISO 26262の
ハザード分析・安全分析との差分分析

本書で分析対象事例とした仮想EPB
(電動パーキングブレーキ)システムの説明

仮想EPBシステムを対象事例とした
STAMP/STPAの試行と効果の抽出

自動車メーカとサプライヤの間での効果的・効
率的な運用をめざした、コントロールストラク
チャ図や分析過程記述の標準化提唱

各社での個別分析事例を紹介(6社)

備考： 各執筆者によるショートコラム「コーヒーブレーク」を含め、約170ページ

(1) JASPAR機能安全WGの全体活動

(2) STAMP/STPAの自動車向け活用ガイドの概要

(3) 自動車用機能安全規格ISO 26262との差分分析

(4) 対象システム事例 (仮想 EPBシステム)

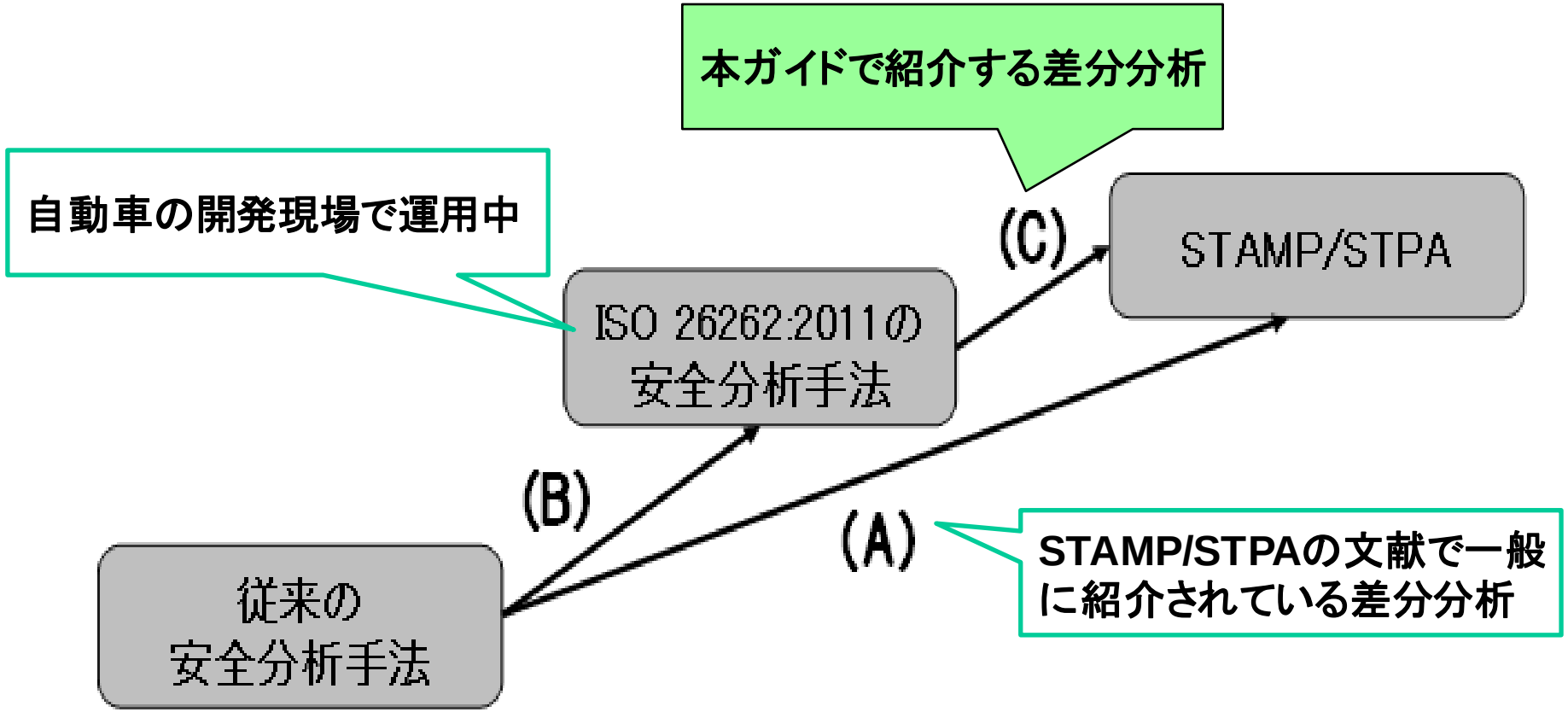
(5) 分析事例

(6) 提唱

(7) まとめ

STAMP/STPAとISO 26262との比較（差分分析）

■自動車用車載制御システムの開発現場からの疑問：
「STAMP/STPAの解説書で従来手法に対する差分が示されているが、ISO 26262で取り組み済と思われるものもある。ISO 26262に対する差分がわかりづらい。」
●JASPAR機能安全WGの対応：
ISO 26262に対してSTAMP/STPAの優位な部位を差分分析し、ガイドに記載



STAMP/STPAとISO 26262との比較（差分分析）

STAMP/STPAとISO 26262:2011を比較すると、STAMP/STPAにもっとも近いと思われるプロセス部位は以下
a) 安全要求の導出と配置
b) システム安全分析（システムFTA/システムFMEAなど）

◆ISO 26262:2011の安全要求の導出とSTAMP/STPAとの比較

	ISO 26262:2011の安全要求の導出	STAMP/STPA
段階（フェーズ）	コンセプト	（明確な規定はないが）コンセプト
構成図（エレメント間や外部とのインタラクションの記載を含む）	アーキテクチャ図にインタラクションも記載されるのが一般的である。ただし、インタラクションの記載に関して規格での明確な規定はない。	コントロールストラクチャ図にインタラクションも記載される。インタラクションを記載するよう明確に規定されている。
手順	1)ハザード分析＆リスクアセスメントおよび安全目標の導出 2)機能安全要求の導出 3)機能安全コンセプト（配置） 4)技術安全要求の導出 5)技術安全コンセプト（配置）	Step 0：（準備1） アクシデント、ハザード、安全制約の識別 Step 0：（準備2） コントロールストラクチャの構築 Step 1：非安全なコントロールアクション（UCA）の抽出 Step 2：ハザード要因（HCF）の特定

STAMP/STPAとISO 26262との比較（差分分析）

◆ISO 26262:2011のシステムFTA/システムFMEAとSTAMP/STPAとの比較

	ISO 26262:2011の システムFTA/システムFMEA	STAMP/STPA
段階（フェーズ）	システム	（同左）
障害の箇所	エレメント間や外部とのインタフェース上に現れる障害（エレメント間や外部とのインタラクション）に着目	（同左）
障害の要因	各エレメントのランダムハードウェア故障やシステマチックフォールトに着目	左記のみでなく、**複数のエレメント間や、人間（ドライバ）、車両などとの相互作用に関わるハザード要因にも着目**
故障モードの分析段階	故障モードは一般的に段階化せずに分析	**故障モードを2段階で分析** **Step 1：非安全なコントロールアクション（UCA）の抽出** （検討対象のコントローラ間のコントロールアクションに着目して抽出する。） **Step 2：ハザード要因（HCF）の特定** 参考文献では、コントロールストラクチャの各コンポーネント間のインタラクションに着目して網羅的に分析する手法が推奨されている。
故障モードのガイドワード、ヒントワード	規格での明確な規定はないが、一般的にHAZOPガイドワードなど利用	**独自のガイドワード、ヒントワードを定義** UCAについては、4つのガイドワードが定義されている。（「与えられない」、「ハザードを誘発する不正内容が与えられる」、「早すぎ、遅すぎ」、など） また、HCFについては、相互作用としてフィードバックへの影響も明記したヒントワードが提案されている。（例：「不適切なフィードバック、あるいはフィードバックの喪失」など）

■差分分析結果：　STAMP/STPAの方が、相互作用（インタラクション）に関わる故障モードを系統的に導出・分析できるよう工夫されている

(1) JASPAR機能安全WGの全体活動

(2) STAMP/STPAの自動車向け活用ガイドの概要

(3) 自動車用機能安全規格ISO 26262との差分分析

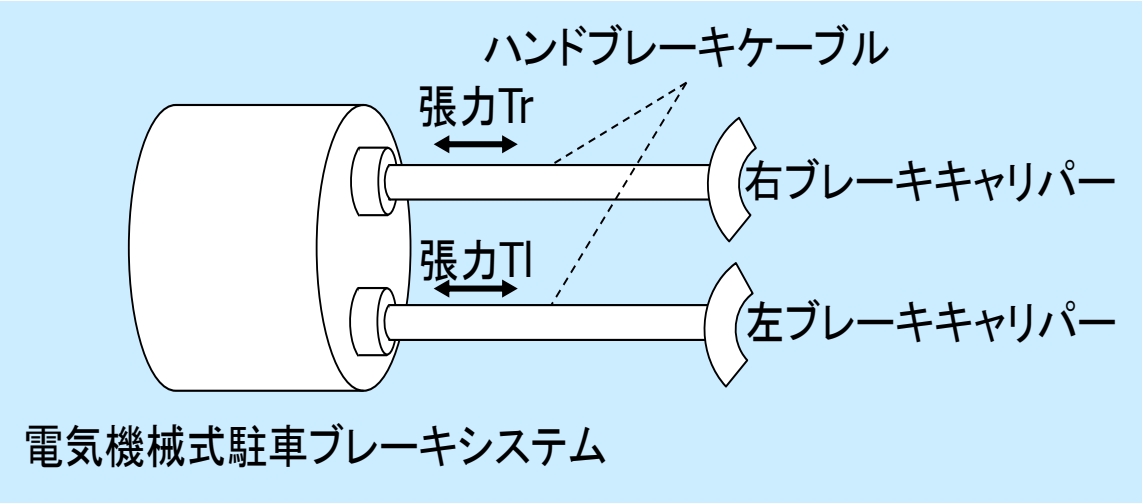
(4) 対象システム事例 (仮想 EPBシステム)

(5) 分析事例

(6) 提唱

(7) まとめ

仮想EPBシステムの機能概要



【目的】
車両停止後に運転者が車両から離れても、既存のブレーキシステムとは独立して車両の停止状態を保持する。
【機能】
・駐車ブレーキスイッチ=ON かつ車速Vf=0(停止)のとき、
傾斜角θに応じた張力TrおよびTlをハンドブレーキケーブルに加えることで、
駐車ブレーキをロックする。
・駐車ブレーキスイッチ=OFFのとき、
張力TrおよびTlを弱めることで、駐車ブレーキを解除する。
・駐車ブレーキのロック／解除状態は表示装置により運転者に通知される。

【備考】 仮想EPBシステムの事例はJASPAR機能安全WG啓蒙活動の一環として作成された14年度教材より引用
文献名称:機能安全技術テンプレート システム開発 技術安全コンセプト編、文献番号:EBP-D-SYS3-001_v101、 作成:OTSL
(仮想EPBシステムを例題に技術安全コンセプトなどが記載されている)

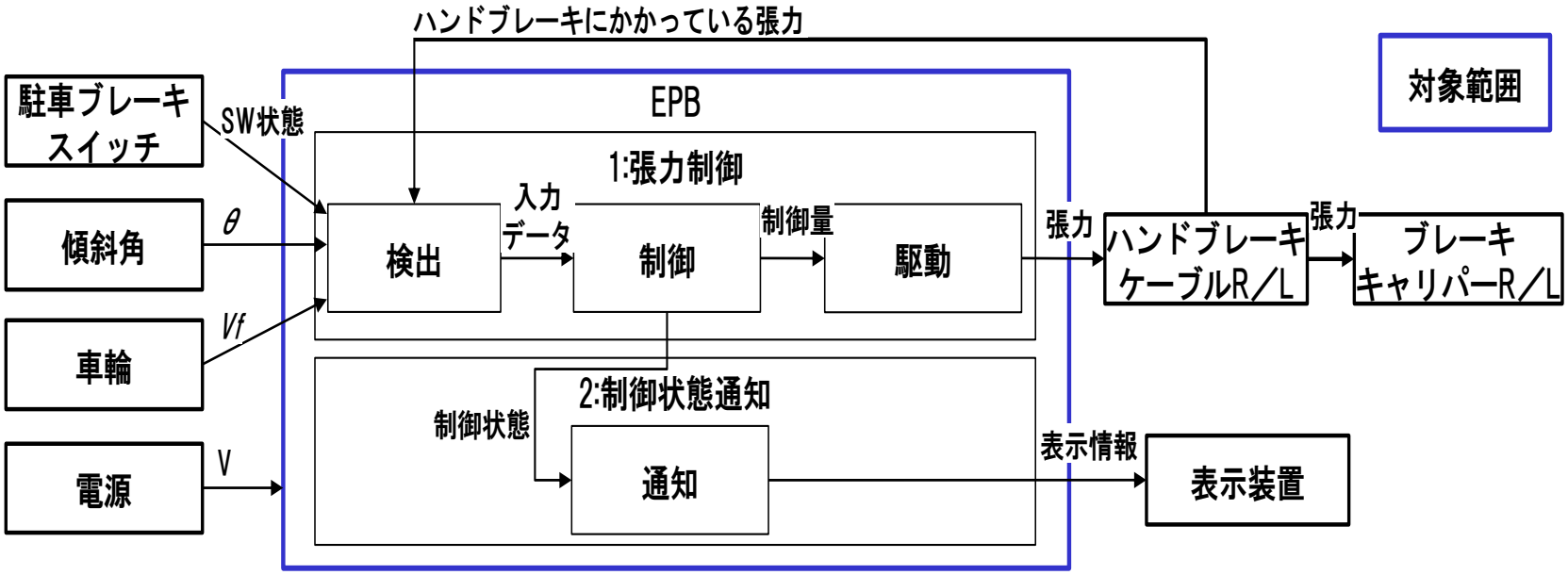
仮想EPBシステムの仕様変更

STAMP/STPAの試行に当たって、仕様変更の影響分析も試行してみたいとの目的から、従来のEPBシステム（前節で説明の基本仕様を有するEPBシステム）から下記に示す制御を変更した。
1）変更前機能：駐車ブレーキスイッチ=OFFになると、駐車ブレーキを解除する
2）変更後機能：駐車ブレーキロック状態で停車中、ドライバがアクセルを踏み込んだ時に、システムが自動で、駐車ブレーキを解除する

◆EPBシステムの基本仕様（仕様変更後）

【目的】
車両停止後に運転者が車両から離れても、既存のブレーキシステムとは独立して車両の停止状態を保持する。
【機能（変更後）】
・駐車ブレーキスイッチ=ON かつ車速Vf=0（停止）のとき、
傾斜角θに応じた張力TrおよびTlをハンドブレーキケーブルに加えることで、
駐車ブレーキをロックする。
・*駐車ブレーキロック状態で、アクセルペダルが踏み込まれたとき*、
張力TrおよびTlを弱めることで、駐車ブレーキを解除する。
・駐車ブレーキのロック／解除状態は表示装置により運転者に通知される。

仮想EPBシステムの機能構成と対象範囲



本図の位置付け:
本図はSTAMP/STPA用の図ではない。ISO 26262と同一レベルから検討開始するために、ISO 26262の適用事例から転載した。

(1) JASPAR機能安全WGの全体活動

(2) STAMP/STPAの自動車向け活用ガイドの概要

(3) 自動車用機能安全規格ISO 26262との差分分析

(4) 対象システム事例 (仮想 EPBシステム)

(5) 分析事例

(6) 提唱

(7) まとめ

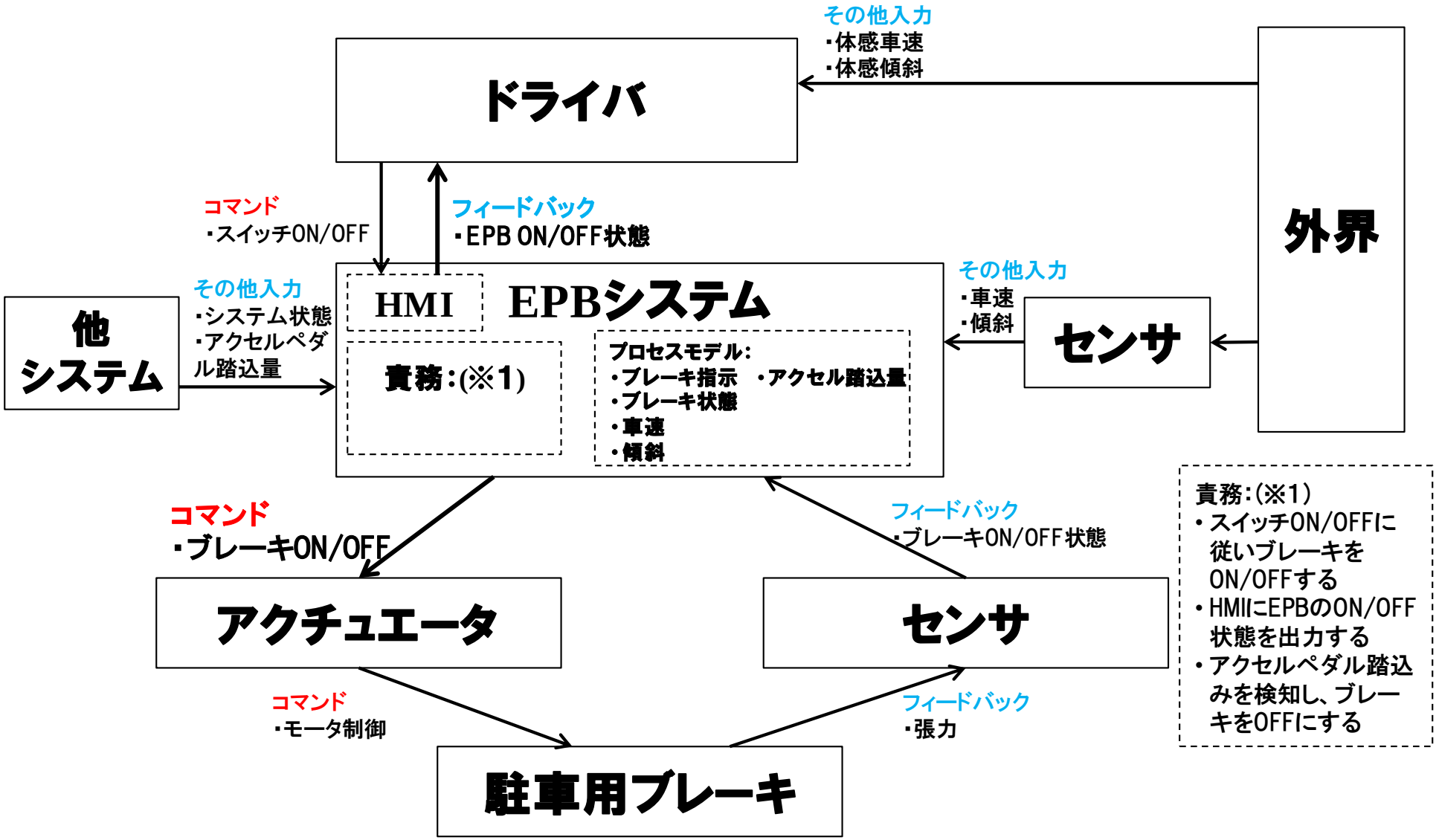
Step０：アクシデント、ハザード、安全制約の識別

アクシデント	ハザード	安全制約
A1:後続車への衝突	H1-1:走行中意図せぬブレーキ力発生	SC1-1:意図せぬブレーキ力を発生させない
	H1-2: ブレーキOFF 状態にもかかわらず、ON 表示しているためドライバが誤って駐車ブレーキスイッチを ON してしまう	*SC1-2:ドライバに誤った情報を提示しない*
A2:坂道下方の障害物への衝突・落下	H2-1:坂道等でブレーキが意図せずかからない	SC2-1:ブレーキ指示時の非作動を発生させない
	H2-2:ブレーキがかかっていない状態で、ブレーキ ON をドライバに通知	SC1-2 に同じ
A3:前方障害物への衝突	*H3-1:アクセル踏み込み後に急なブレーキリリース*	*SC3-1:アクセル踏み込み時には遅滞なくブレーキをリリースする*

黒字：初回検討時に抽出

赤字：後段のプロセスで検討の結果、追加

Step 0: コントロールストラクチャ図（CS図）の作成



Step 1：UCAの抽出

#	制御行動	Not providing	Providing causes hazard	Too early/ Too late	Stop too soon/ Apply too long
1	ブレーキ ON	UCA1:停車時にブレーキがかからない [SC2-1 違反]	UCA2:走行中にブレーキ発生 [SC1-1 違反]	UCA3:(late)停車時にブレーキがかかるのが遅く、傾斜により走行 [SC2-1 違反]	((long)走行開始時にブレーキが解除されない)
2	ブレーキ OFF	－	UCA4:停車中に開放され、傾斜により走行 [SC2-1 違反]	*UCA5:(late)走行開始時にブレーキが遅くに開放され、意図せぬ急加速発生（ドライバがアクセルをさらに強く踏み込むなど） [SC3-1 違反]*	－
3	EPB ON 状態通知	(停車時にドライバが再操作をしてしまう)	*UCA6:走行中にドライバが誤操作をしてしまう[SC1-2 違反]*	((late)停車時にドライバが再操作をしてしまう)	－
4	EPB OFF 状態通知	UCA7:停車時に解除に気付かず、走行 [SC1-2 違反]	－	((late)走行開始時に再操作をしてしまう)	－

赤字：ハザードが追加になった UCA

括弧：非ハザード事象

Step 2: HCFの特定

Step2： HCFの特定の方法として下記が存在

方法A） Causal factorとシナリオを一緒に分析する方法
UCAから事象の連鎖を逆方向にたどり、causal factorに対する解釈を連鎖することで、シナリオを特定する。An STPA Primerで推奨されている方法であり、プロジェクトでの実施例も多い。

方法B） UCAと11個のヒントワードの対応表を作り、causal factorを識別する方法
シナリオを作成する前にcausal factorの洗い出しを実施する。

⇒本ガイドでは、A)とB)のそれぞれの方法を試行した結果を掲載した。

方法A（シナリオ分析）

UCA1: 停車時にブレーキがかからない

なぜ？

1　ドライバがブレーキスイッチを ON にしているにもかかわらず、EPB システムが、ブレーキスイッチ ON コマンドが与えられていることを認識しない。

なぜ？

(ア) ON コマンドの入力が与えられない、あるいは、OFF コマンドとして与えられる。

なぜ？

(ア) ブレーキスイッチの故障、あるいは、割込みコントローラの故障。

(イ) ソフトウェアが ON コマンドを OFF コマンドだと認識している。

なぜ？

(ア) ソフトウェアの実装ミス、あるいは、CPU などのハードウェア故障による演算誤り。

方法B（ヒントワードによる対応表）

UCA/原因分類	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
	・コントロール入力の外部情報が欠けているか間違っている	・不適切なコントロールアルゴリズム	・不整合、不完全、または不正確なプロセスモデル ・不適切な操作	・コンポーネント不具合 ・経年による変化	・不適切なフィードバック ・フィードバックの喪失 ・フィードバック遅れ	・不正確な情報供給 ・情報欠如 ・測定不正確性 ・フィードバック遅れ	・操作遅れ	・不適切または無効なコントロールアクション ・コントロールアクション喪失	・コントロールアクションの衝突 ・プロセス入力喪失または誤り	・未確認、または範囲外の障害	・システムにハザードを引き起こすプロセス出力
UCA1:停車時にブレーキがかからない	・スイッチ ON が正しく伝達されない ・誤ったアクセル踏込情報入力	・コントローラ内部演算誤り	・コントローラ内部演算誤り	・ブレーキ故障 ・許容範囲外の高温・低温	・誤ったブレーキ ON 状態通知	・張力値が正しく伝達されない	・モータ制御値が正しく伝わらない	・ブレーキ ON 指示が正しく伝わらない	—	—	—
UCA2:走行中にブレーキ発生	・誤ったスイッチ ON 入力	・コントローラ内部演算誤り（ブレーキ指示・ブレーキ状態）	・コントローラ内部演算誤り（ブレーキ指示・ブレーキ状態）	・ブレーキ故障 ・許容範囲外の高熱・低温	—	—	・誤ったモータ制御値送信	・誤ったブレーキ ON 送信	—	—	—

試行結果考察とSTAMP/STPAの効果

◆UCAの抽出

UCAの抽出過程において、当初考慮していなかったハザードを摘出できた。
- UCA5：タイミングに関するガイドワード「Too early/too late」と、
  ユーザ（ドライバ）との相互作用の検討から抽出
- UCA6：ユーザ（ドライバ）との相互作用の検討から抽出

STAMP/STPAの効果：相互作用やタイミングに関わる不具合動作を抽出容易化

◆HCFの特定

	方法A（シナリオ記述）	方法B（ヒントワードによる対応表）
長所	「なぜ、なぜ、なぜ」と続けることで、原因までつきとめることができる。	HCFのヒントワード（原因分類）があるので、検討が容易である。 次に何をすれば良いか悩まずに済む。
短所	網羅性が分かりづらい。 後に何らかの方法でまとめる作業が必要となる。	全ての項目を埋める（考える）コストが必要となる。 表を埋めることが目的になり、自由な発想による多様な検討が行われないリスクがある。

STAMP/STPAの効果：相互作用に関わる原因特定方法を具体化・明確化

(1) JASPAR機能安全WGの全体活動

(2) STAMP/STPAの自動車向け活用ガイドの概要

(3) 自動車用機能安全規格ISO 26262との差分分析

(4) 対象システム事例 (仮想 EPBシステム)

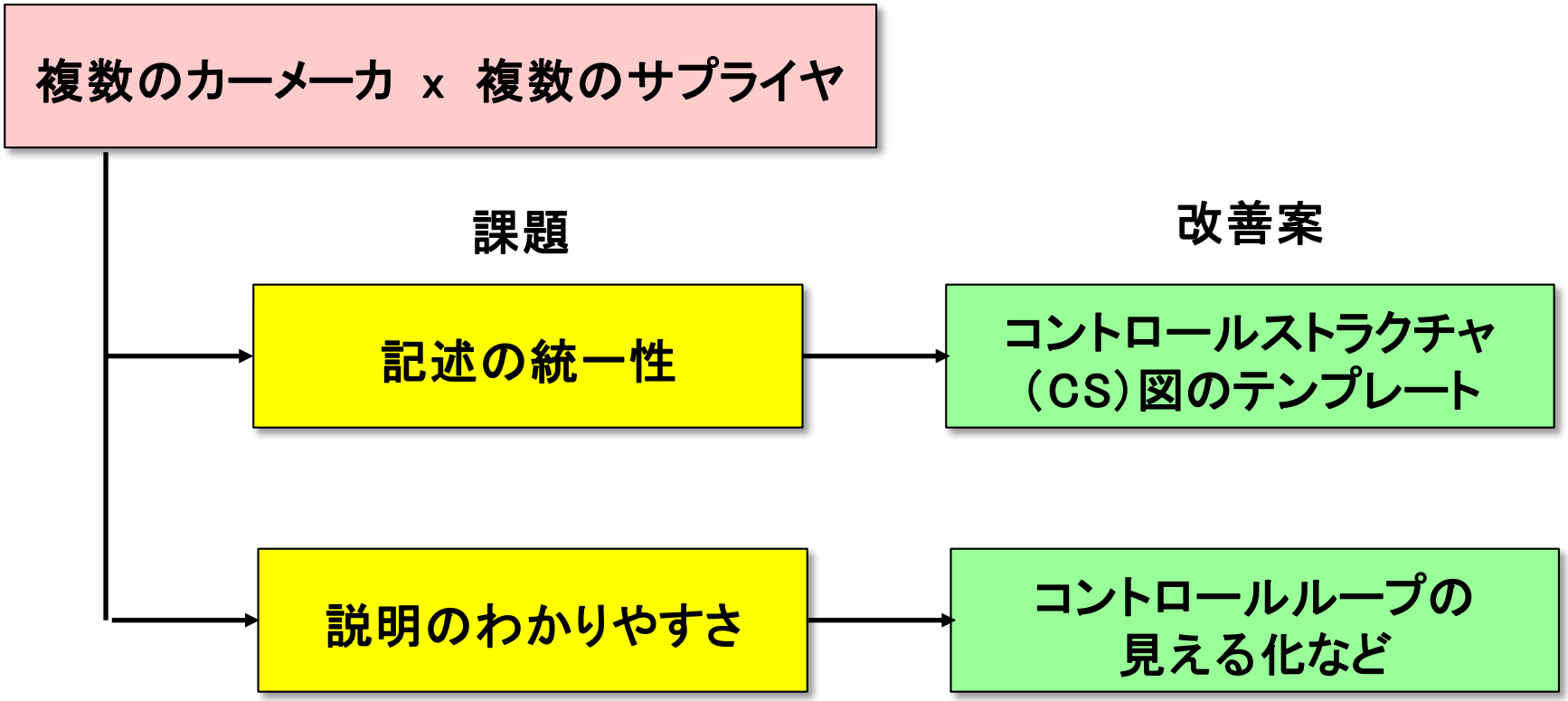
(5) 分析事例

(6) 提唱

(7) まとめ

STAMP/STPA活用上の課題と改善案

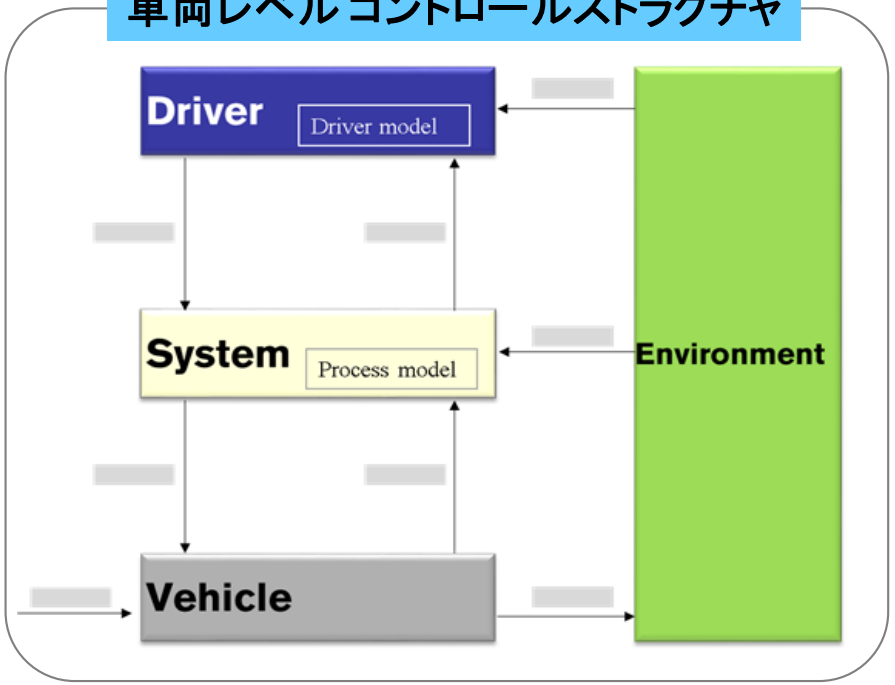
背景： 自動車業界のビジネス形態



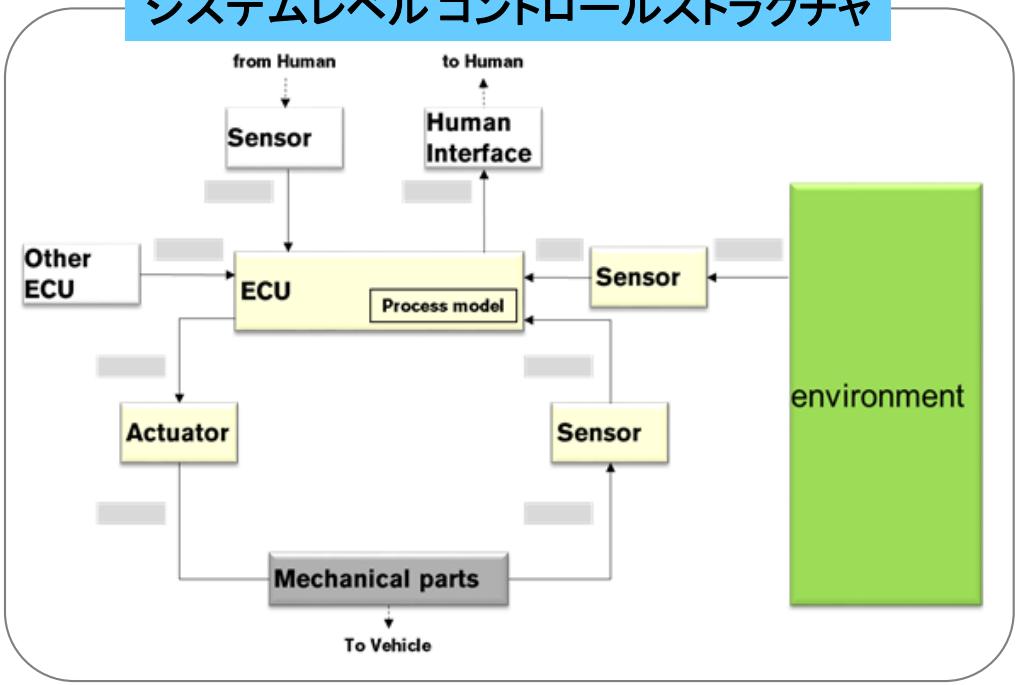
コントロールストラクチャ(CS)図のテンプレート

◆目的
コントロールストラクチャ(CS)図の記述の標準化
◆特徴
（1）車両レベル（上位）＋システムレベル（下位）の階層的コントロールストラクチャ
（2）総合視点を取り入れた「車両レベル コントロールストラクチャ」
　　大規模システムで考慮すべき、人／システム／環境／車両をコンポーネントとした。
（3）開発役割分担を考慮した「システムレベル コントロールストラクチャ」
　　自社に関係する部分／しない部分が分かるようコンポーネントの凡例を分けた。

車両レベル コントロールストラクチャ

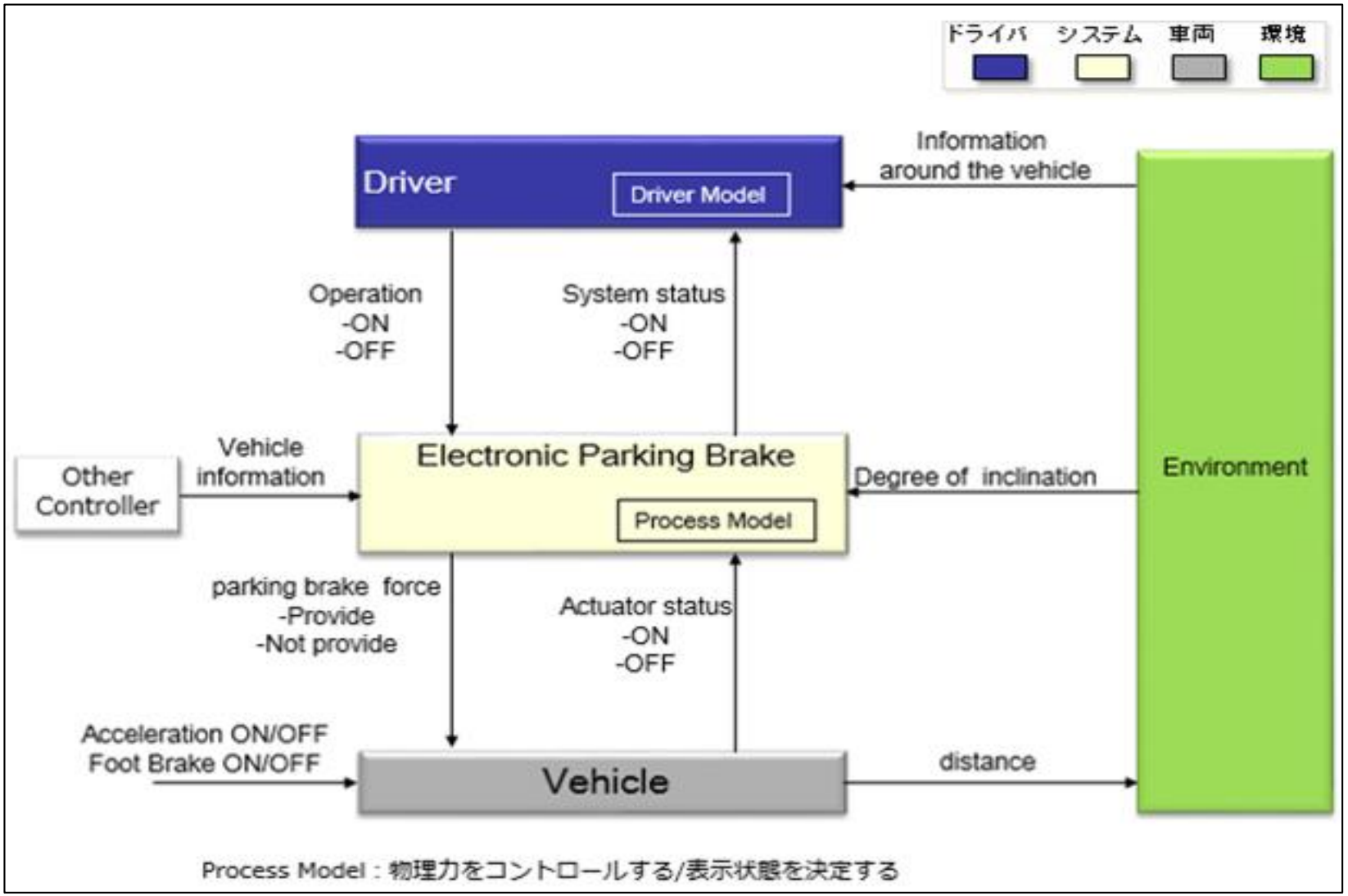


システムレベル コントロールストラクチャ



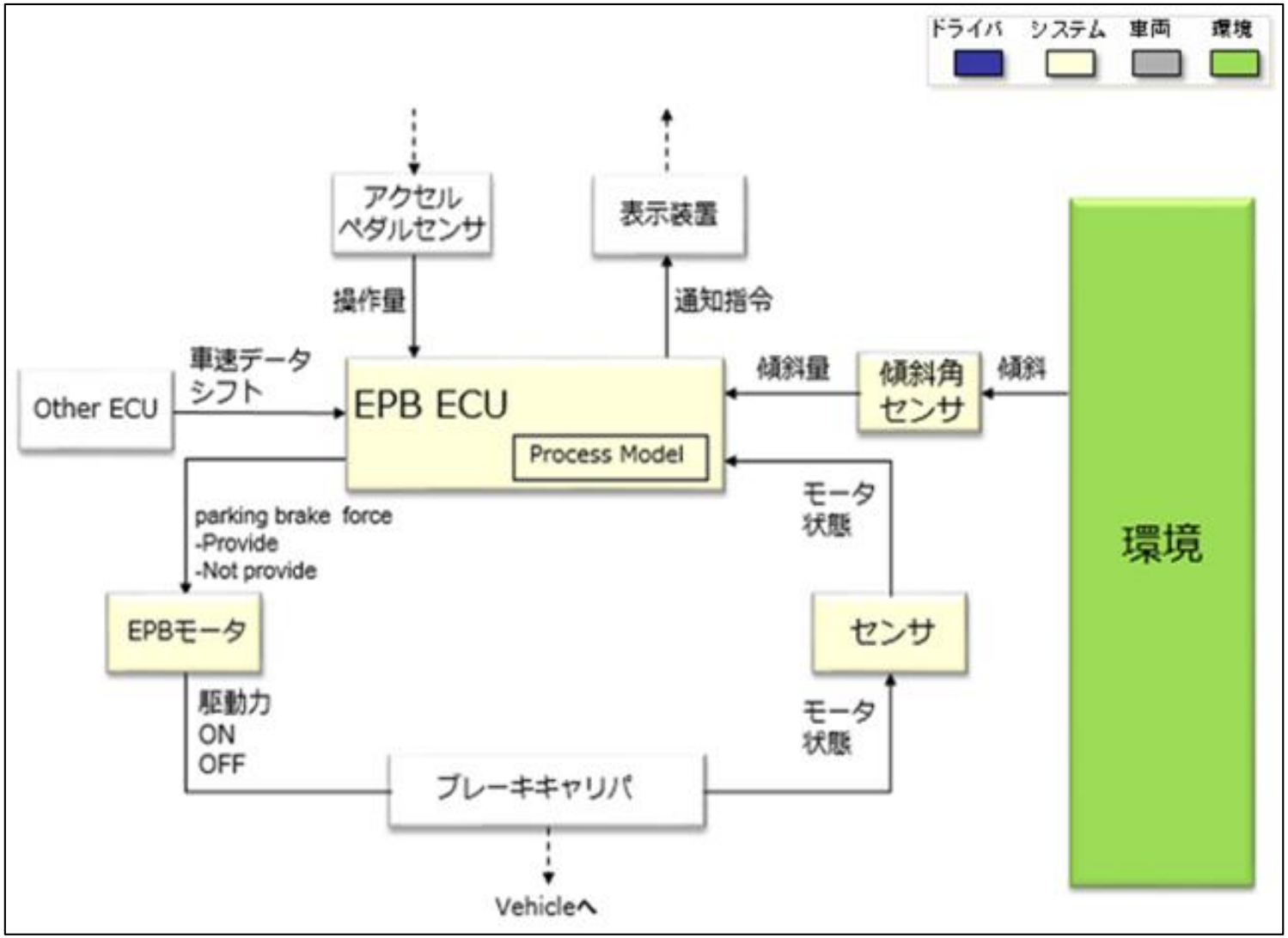
コントロールストラクチャ(CS)図の記載例(1)

仮想EPBシステムの車両レベル コントロールストラクチャ



コントロールストラクチャ(CS)図の記載例(2)

仮想EPBシステムのシステムレベルコントロールストラクチャ



コントロールループの見える化(1)

◆目的
「STEP1：UCAの抽出」における 網羅性の説明および影響分析の理解促進
◆特徴
（1）すべてのコントロールアクションに対してSTPAガイドワードを当てはめた分析結果を一覧化
（2）コントロールストラクチャ上にUCAやその影響を矢印（コントロールループ）で記載

STEP1

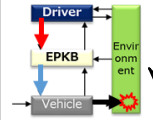
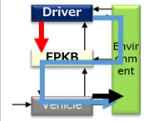
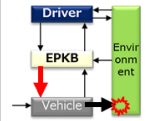
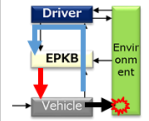
手順

UCAの抽出

Control action	NP	P	T	D
Turn parking switch on	CA1-NP1 Driver does not turn the parking switch on while vehicle is stopping on the slope.	CA1-P1 Driver turn the parking switch on while vehicle is running.	CA1-T1 Driver turn the parking switch on before vehicle stop. CA1-T2 Driver turn the parking switch on too late while vehicle is stopping on the slope.	CA1-D1 Driver stop turning the parking switch on too soon while vehicle is stopping on the slope.
Turn parking switch off	-	CA1-P2 Driver turn the parking switch off while vehicle is stopping on the slope.	-	-

改善

分析結果一覧
コントロールループの見える化

Control structure	Description	Related UCA
	Driver turn the parking switch on while vehicle is running. Driver turn the parking switch on before vehicle stop.	CA1-P1 CA1-T1
	...stopping on the slope.	CA1-P2
	...icle is stopping on the	CA1-T2
	Driver ...hicle is stopping on the slo	CA1-NP1
	EPB ...hicle is stopping on the slo	CA2-NP1
	EPB re...opping on the slope.	CA2-P2
	EPB pro...	CA2-T2
	EPB releases parking brake lock after driver get out the car on the slope.	CA2-T3
	EPB provides parking brake force while vehicle is running.	CA2-P1
	EPB provides parking brake force before vehicle stop.	CA2-T1
	EPB release parking brake lock too late.	CA2-T4

コントロールループの見える化(2)

◆目的
「STEP2: HCFの特定と安全要求の導出」における 分析結果の理解促進
◆特徴
（1）階層別にシナリオベース分析
（2）コントロールストラクチャ上にUCAやその影響を矢印（コントロールループ）で記載

STEP2

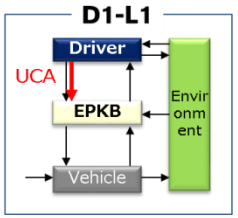
手順

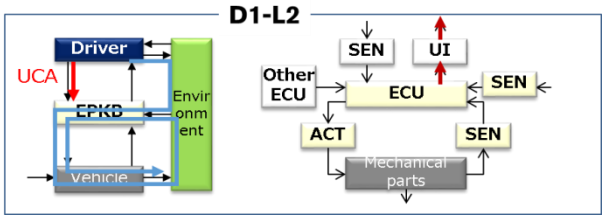
HCFの特定と
安全要求の導出

Loop	Scenario	Reg ID	Contents
D1-L1	Driver believes that EPB system is "ON", but system is really "OFF". Then Driver gets out of the car without EPB "ON". This could lead to the "Accident 1, 2 or 3". (1miss)	SR1	EPB system shall alert to the driver in the following condition; ● EPB OFF and ● Shift is not "P" or "R" and Sheet belt OPEN or Door Open
D1-L2	Driver believes that EPB system is "ON", because system display "ON", but system is really "OFF". Then Driver gets out of the car without EPB "ON". This could lead to the "Accident 1, 2 or 3". (1Failure plus miss)		

改善

階層別にシナリオベース分析
コントロールループの見える化





Loop	Causal Scenario	Safety Requirements
D1-L1	Driver believes that EPB system is "ON", but system is really "OFF". Then Driver gets out of the car without EPB "ON". This could lead to the "Accident 1, 2 or 3". (1miss)	Safety requirement 1 EPB system shall alert to the driver in the following condition; ● EPB OFF and ● Shift is not "P" or "R" and ● Sheet belt OPEN or Door Open
D1-L2	Driver believes that EPB system is "ON", because system display "ON", but system is really "OFF". Then Driver gets out of the car without EPB "ON". This could lead to the "Accident 1, 2 or 3". (1Failure plus miss)	

(1) JASPAR機能安全WGの全体活動

(2) STAMP/STPAの自動車向け活用ガイドの概要

(3) 自動車用機能安全規格ISO 26262との差分分析

(4) 対象システム事例（仮想 EPBシステム）

(5) 分析事例

(6) 提唱

(7) まとめ

まとめ

◆クルマの電子制御化は、自動運転も視野に入れつつ、急速に進化中。自動運転では複数のシステムが連携する大規模かつ複雑なシステムとなる。従来の安全分析(FTA, FMEA)のみでは見落としのリスクがあり、STAMP/STPAの活用が有効と考えられる。
◆JASPAR機能安全WGでは、STAMP/STPAを開発現場で効果的・効率的に活用できないかを検討し、開発現場向けに活用ガイドとして纏めた。その主な内容は、以下である。
（1）すでに運用中のISO 26262のハザード分析・安全分析との差分分析
（2）仮想EPB(電動パーキングブレーキ)システムを対象事例としたSTAMP/STPAの試行と効果の抽出
（3）複数の関係者の間での記述の統一性や理解促進を目的に、コントロールストラクチャ図のテンプレートやコントロールループの見える化を提唱

【ご参考】

今回紹介の「STAMP/STPA活用ガイド～自動車編～」は’17年10月に公開済（JASPAR会員向け）
（ガイド入手希望される方でJASPAR未加入の場合は、JASPARへのご加入を検討ください）
また、その内容の一部は、独立行政法人情報処理機構(IPA)の公開資料でも紹介いただく予定

ご清聴ありがとうございました

以上