HITACHI
Inspire the Next

第2回　STAMPワークショップ

自動運転系の安全・セキュリティ解析のための自動化ヒューマンファクタに基づくSTPAガイドワードの提案

2017/11/28

株式会社 日立製作所　サービスプラットフォーム事業本部
セキュリティ事業統括本部

永井康彦

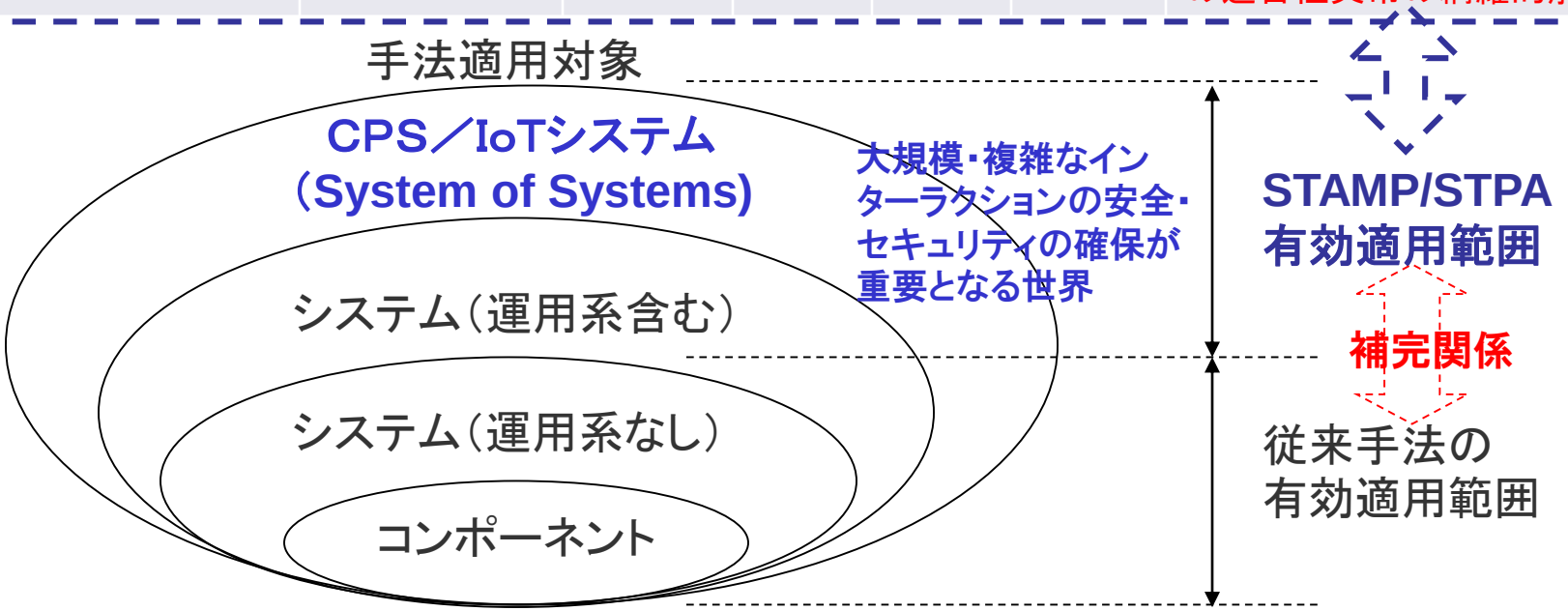
HITACHI
Inspire the Next

Contents

1-1. 背景(なぜ今STAMP/STPAなのか？)

HITACHI
Inspire the Next

根本的相違点 / 手法	解析の焦点	解析のタイプ	解析のアプローチ	解析所要時間	解析の担当者	有効用途
従来手法（FMEA、FTA手法等）	コンポーネント異常	ブラックリスト型	狭く・深く	長期	専門家	コンポーネント故障・異常の深い解析
STAMP/STPA手法	コンポーネント間のインターラクション異常	ホワイトリスト型	広く・浅く	短期	一般エンジニアも可	大規模・複雑なシステムのコンポーネント異常に起因しないシステム動作や人・環境との適合性異常の網羅的解析



出典；SCIS2016 「新システムセキュリティ解析手法STAMP/STPAの有効性に関する一考察」永井・福澤発表資料

1-2. 背景(なぜ今STAMP/STPAなのか？)

HITACHI
Inspire the Next

- 従来手法により個々のコンポーネント機器の信頼性・安全性は向上
- 現代の障害・脅威の大多数はそれ以外の原因(人的、組織的、運用的、環境的不適合や安全制約違反)で発生している問題
  - 故障はないのに事故、ソフトウエアはそもそも故障はしない⇒安全要件・設計の不備
  - 事例;
    - 福島第一原発の電源喪失事故
    - 福知山線の脱線事故
    - 中部国際空港の中華航空機墜落事故
    - ベネッセ、日本年金機構の個人情報漏えい事件
- **今後のネットワーク・ソフトウエア化、システム間連携、組織・制度とも連携した社会技術システムに対して、コンポーネント間相互作用の複雑性を捉え、相互連携部分で生ずる障害・脅威への対策(システム特性領域)が重要！**

あらゆるモノがネットワーク化・ソフトウエア化される動向の社会技術システムが中心・依存の世界に突入

安全に対する考え方のパラダイムシフトが必要
(コンポーネント信頼性の従来手法⇒システム特性領域の問題を扱うのに適した手法が必要)

STAMP/STPA手法は、今後のIoT/CPS時代の
システム安全・システムセキュリティ確保のための核となる解析手法として有効・有望

出典;SCIS2016「新システムセキュリティ解析手法STAMP/STPAの有効性に関する一考察」永井・福澤発表資料

1-3. 本研究の目的

HITACHI
Inspire the Next

STAMP(Systems-Theoretic Accident Model and Process):システム理論に基づく事故モデル
STPA(STAMP based Process Analysis):STAMPに基づく安全解析手法

期待

- IoT/CPS時代、特に、今後増加が予想される**AI等応用した自動化システムの監視制御系(SVC;スーパーバイザリコントロールシステム)のMMI(マンマシンインターラクション)環境のヒューマンファクタ問題の解決のためにSTPA利用**の解析が有効
- 自動化システムへの適用例(自動運転系)
  - STAMP Workshop 2016;"AUTOMOBILE FEATURES FOR LANE MANAGEMENT"
  - STAMP Workshop 2017;"Evolution Issues of Automated Driving Functions by Application of Systemic Accident Analysis : On the Example of the Tesla Model S Fatality"
  - STAMP Workshop 2017;" ENGINEERING FOR HUMANS Human-Automation Interaction in STPA" 等

課題

- STPA手法でハザード/UCA(不安全コントロールアクション)の要因(CF:Casual Factor)特定に用いる**現状の基本CFガイドワードは、汎用過ぎてSVC系ヒューマンファクタ問題の要因を一般的エンジニアが適切な粒度で網羅的に抽出することは困難**

目的

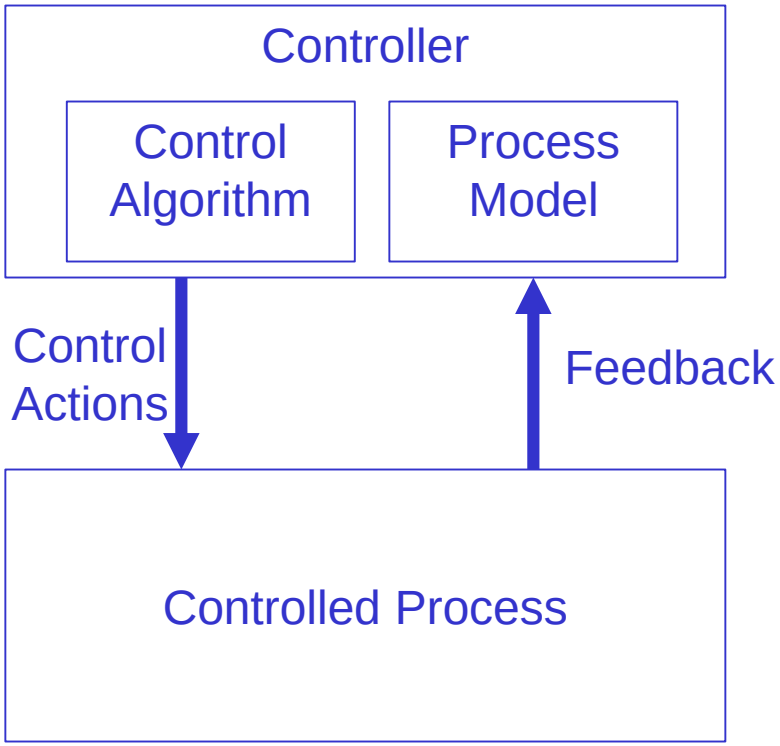
- 今後のIoT/CPSの中でも、AI応用の知的システム利用において重要課題となる、人間とのインターラクション異常分析へのSTPAを有効活用できるよう、先行航空分野のSVC系ヒューマンファクタの知見をベースに、**SVC系解析向けにクラス階層構造化して対象に応じて特化して利用することで、容易にSVCヒューマンファクタ要因を抽出可能とするガイドワードを提案**

2-1. STAMPの概要

HITACHI
Inspire the Next

- STAMP(Systems-Theoretic Accident Model and Process)とは？
  - システム理論(トップダウンアプローチ)に基づく新たな事故モデル
  - 解析対象を、階層構造の**制御プロセスモデル(コントロールストラクチャ)**としてモデル化し、モデル要素間の相互作用が安全性制約を逸脱した結果によって事故が発生すると考える。

＜ **Safety Control Structureの基本構成** ＞



2-2. STPAの手順とCFガイドワードの位置づけ

HITACHI
Inspire the Next

STPA(STAMP based Process Analysis);STAMPに基づくハザード分析(安全解析)手法

開始

【準備1】
アクシデント、ハザードの設定

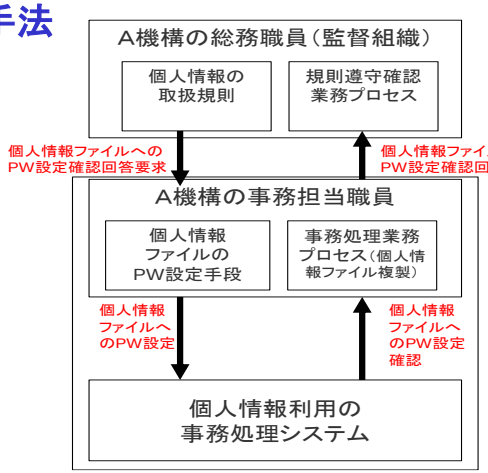
解析対象とするシステムのアクシデントやハザード(脅威・脆弱性)を設定

アクシデント;喪失を伴うシステムの事故
ハザード;アクシデントにつながるシステムの状態

【準備2】
コントロールストラクチャの構築

設定ハザードに関するコントロールストラクチャ作成

コントロールプロセスモデルとアルゴリズム(手順)を含むコントローラとコントロールドプロセス間でコントロールアクションとフィードバックのコントロールループがある制御プロセスモデル



【分析1】
不安全コントロールアクション(UCA)の識別

ハザードにつながる恐れのあるUCAを識別

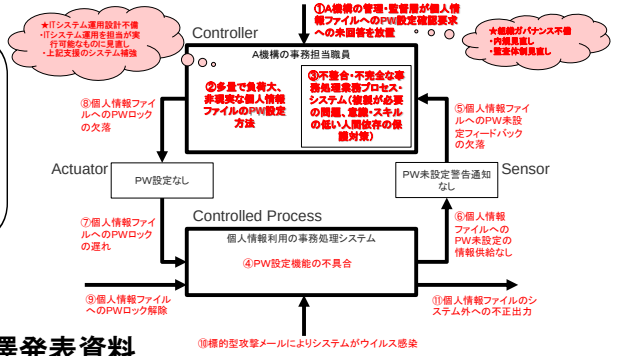
コントロールループのコントロールアクションとフィードバックについて4個のガイドワードで抽出・識別

IFポイント	From ⇒To	Control Action / Feed Back	4個のガイドワード			
			①Not providing	②Unsafe control action	③Too early, too late, out of sequence	④Stopping too soon or continuing too long
A機構の事務担当⇔情報系事務処理システム(H⇔Mインターラクション)	事務担当⇒事務処理システム	個人情報ファイルへのPW設定	担当者のPW設定非順守	ポリシー違反のPW設定	事後設定	フォローアップ不備(共有サーバへの長期間保存)
	事務処理システム⇒事務担当	個人情報ファイルへのPW設定確認	管理者による確認なしシステムからPW設定確認非通知	偽確認通知	通知遅延	通知忘却
A機構の総務職員(監督組織)⇔事務担当(O⇔Hインターラクション)	総務⇒事務担当	個人情報ファイルへのPW設定確認回答要求	要求未伝達	懲罰・強制力のない要求(努力目標化)	事後要求	フォローアップ不備(監査対象外)
	事務担当⇒総務	個人情報ファイルへのPW設定確認回答	未回答・無視	虚偽回答	回答遅延	回答忘却・放置

【分析2】
誘発要因(CF)の特定

分析1で識別したUCAの原因となるCFを特定

コントロールループのUCAのCFを11個のガイドワードで特定し、CFを制御・除去するための安全制約を導出



UCA;Unsafe Control Action, CF;Casual Factor

終了

出典;SCIS2016「新システムセキュリティ解析手法STAMP/STPAの有効性に関する一考察」永井・福澤発表資料

2-3. STPA【分析2ステップ】; ①～⑪11個の要因CF抽出のガイドワード一覧

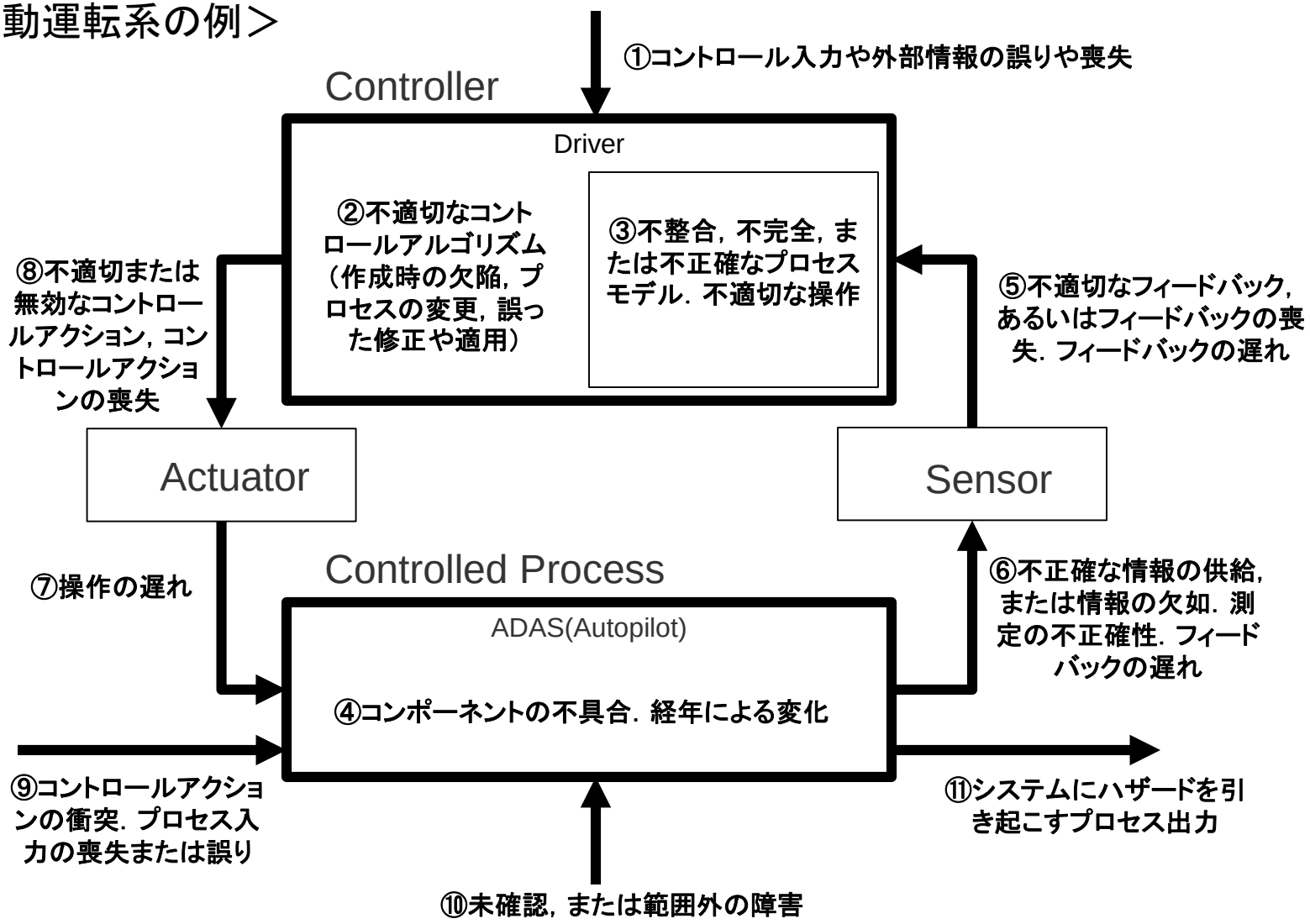
HITACHI
Inspire the Next

① コントロール入力や外部情報の誤りや喪失.
② 不適切なコントロールアルゴリズム(作成時の欠陥, プロセスの変更, 誤った修正や適用).
③ 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.
④ コンポーネントの不具合. 経年による変化.
⑤ 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. フィードバックの遅れ.
⑥ 不正確な情報の供給, または情報の欠如. 測定の不正確性. フィードバックの遅れ.
⑦ 操作の遅れ.
⑧ 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の喪失.
⑨ コントロールアクションの衝突. プロセス入力の喪失または誤り.
⑩ 未確認, または範囲外の障害.
⑪システムにハザードを引き起こすプロセス出力.

2-4. 11個の要因CFのコントロールループ図上の位置づけ

HITACHI
Inspire the Next

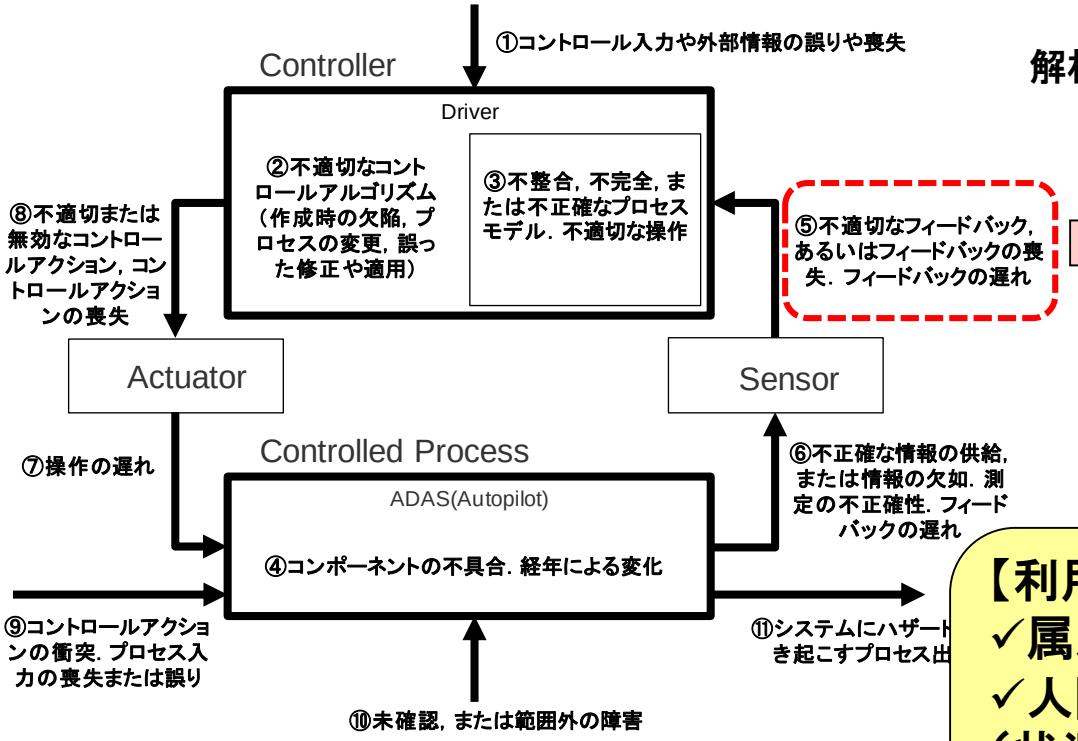
＜自動運転系の例＞



ADAS；Advanced Driver-Assistance Systems

2-5. 現状CFガイドワードの利用上の問題点

HITACHI
Inspire the Next



SVC系ヒューマンファクタ
（例；自動運転）に適用

解析対象・問題分野に特化・カスタマイズして利用

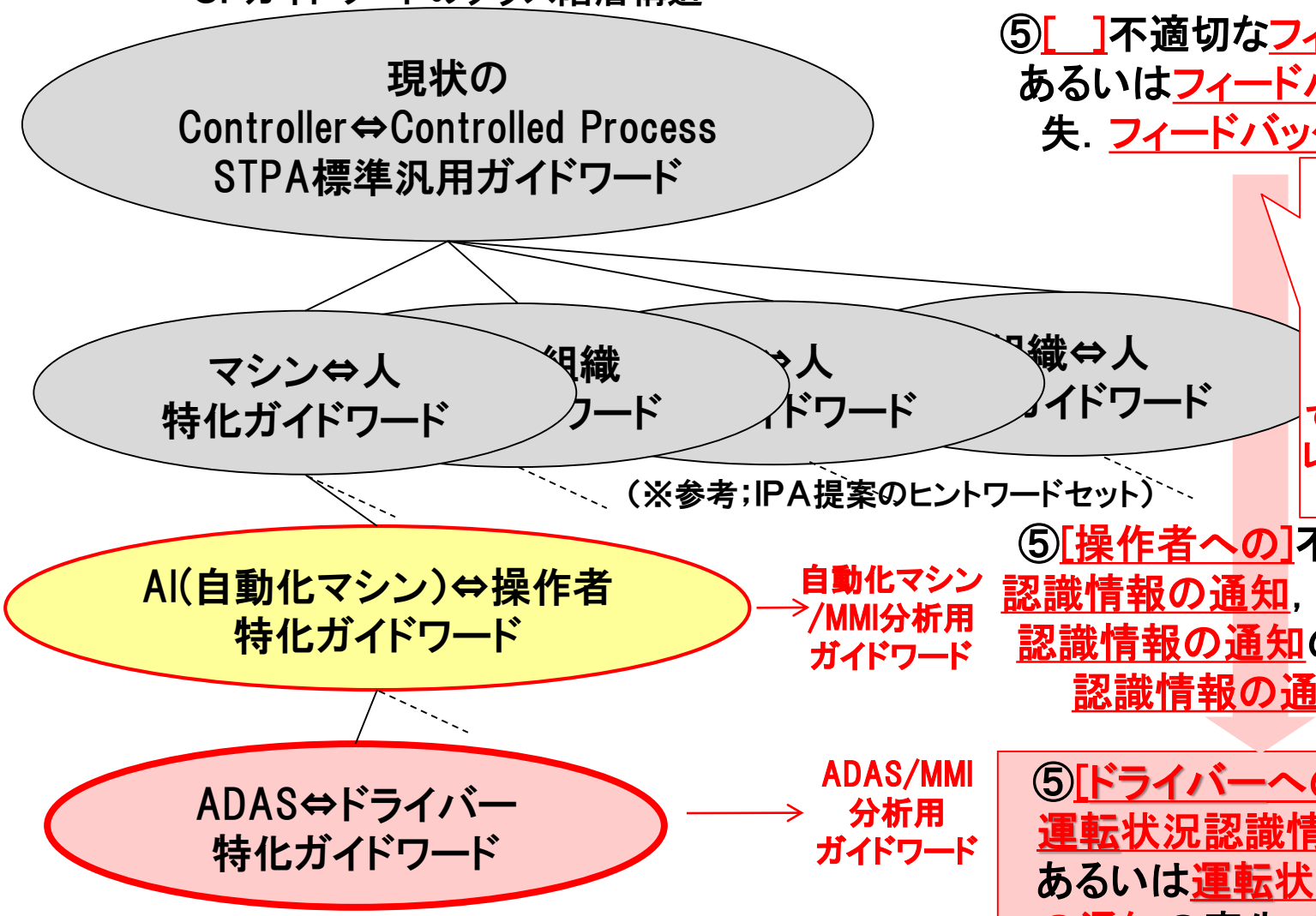
⑤ドライバーへの不適切な運転状況認識情報の通知、あるいは運転状況認識情報通知の喪失、運転状況認識情報通知の遅れ．

【利用上問題点】
✓属人性が高い（解析者スキルに依存）
✓人間工学、認知工学分野の専門知識（状況認識の喪失など）が必要
⇒一般エンジニアではSVC系ヒューマンファクタのCFを特定困難

3-1. CFガイドワードの階層的クラス構造化定義の提案

HITACHI
Inspire the Next

CFガイドワードのクラス階層構造



（※参考；IPA提案のヒントワードセット）

構造化ガイドワード定義例

⑤[　]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．フィードバックの遅れ

[xxx];割付・具体化
yyy;詳細化
による特化操作を、
・コントロールループ種別
・分野/対象共通
・分野/対象個別
で段階的、階層的に各レベルのガイドワードを定義

⑤[操作者への]不適切な状況認識情報の通知，あるいは状況認識情報の通知の喪失．状況認識情報の通知の遅れ

⑤[ドライバーへの]不適切な運転状況認識情報の通知，あるいは運転状況認識情報の通知の喪失．運転状況認識情報の通知の遅れ

ADAS；Advanced Driver-Assistance Systems
MMI；Man-Machine Interaction

3-2. 自動化の段階レベルと現状ADASレベル

HITACHI
Inspire the Next

制御主体	段階レベル	レベル定義
人間主体	(1)	コンピュータの支援なしに、すべてを人間が決定・実行
	(2)	コンピュータはすべての選択肢を提示し、人間はそのうちのひとつを選択して実行
	(3)	コンピュータは可能な選択肢をすべて人間に提示するとともに、その中のひとつを選んで提案、それを実行するか否かは人間が決定
	(4)	コンピュータは可能な選択肢の中からひとつを選び、それを人間に提案、それを実行するか否かは人間が決定
	(5)	コンピュータはひとつの案を人間に提示、人間が了承すれば、コンピュータが実行
コンピュータ優先	**(6)**	**コンピュータはひとつの案を人間に提示、人間が一定時間以内に実行中止を指令しない限り、コンピュータはその案を実行**
	(6.5)	コンピュータはひとつの案を人間に提示すると同時に、その案を実行
	(7)	コンピュータがすべてを行い、何を実行したか人間に報告
	(8)	コンピュータがすべてを決定・実行、人間に問われれば、何を実行したか人間に報告
	(9)	コンピュータがすべてを決定・実行、何を実行したか人間に報告するのは、必要性をコンピュータが認めたときのみ
	(10)	コンピュータがすべてを決定し、実行

現状ADASのレベル
（自動運転レベル2、3）
⇒SVC系
ドライバーの役割は運転から監視・監督中心へ

参考;「人と機械の共生のデザイン」稲垣、森北出版(2012)

3-3. 先行航空分野の自動化ヒューマンファクタ問題の知見整理

HITACHI
Inspire the Next

＜自動化(SVC系)におけるヒューマンファクタ(HF)問題＞

参考;「人と機械の共生のデザイン」稲垣、森北出版(2012)

[監視(認知)系]

(a)状況認識の喪失

- 自動化システムの機能・論理や作動・異常状態が把握困難、オートメーションサプライズ、意図の対立

[判断系]

(b)退屈、危機感の喪失

- 自動化による低すぎるワークロード、人の周辺化

(c)不信、規則違反

- 自動化システムを使うべき時に使わない

(d)過信、過度の依存、規則違反

- 自動化システムを使ってはいけない時に使う

(e)不測事態対応不能:アップセットリカバリ能力の低下・欠如

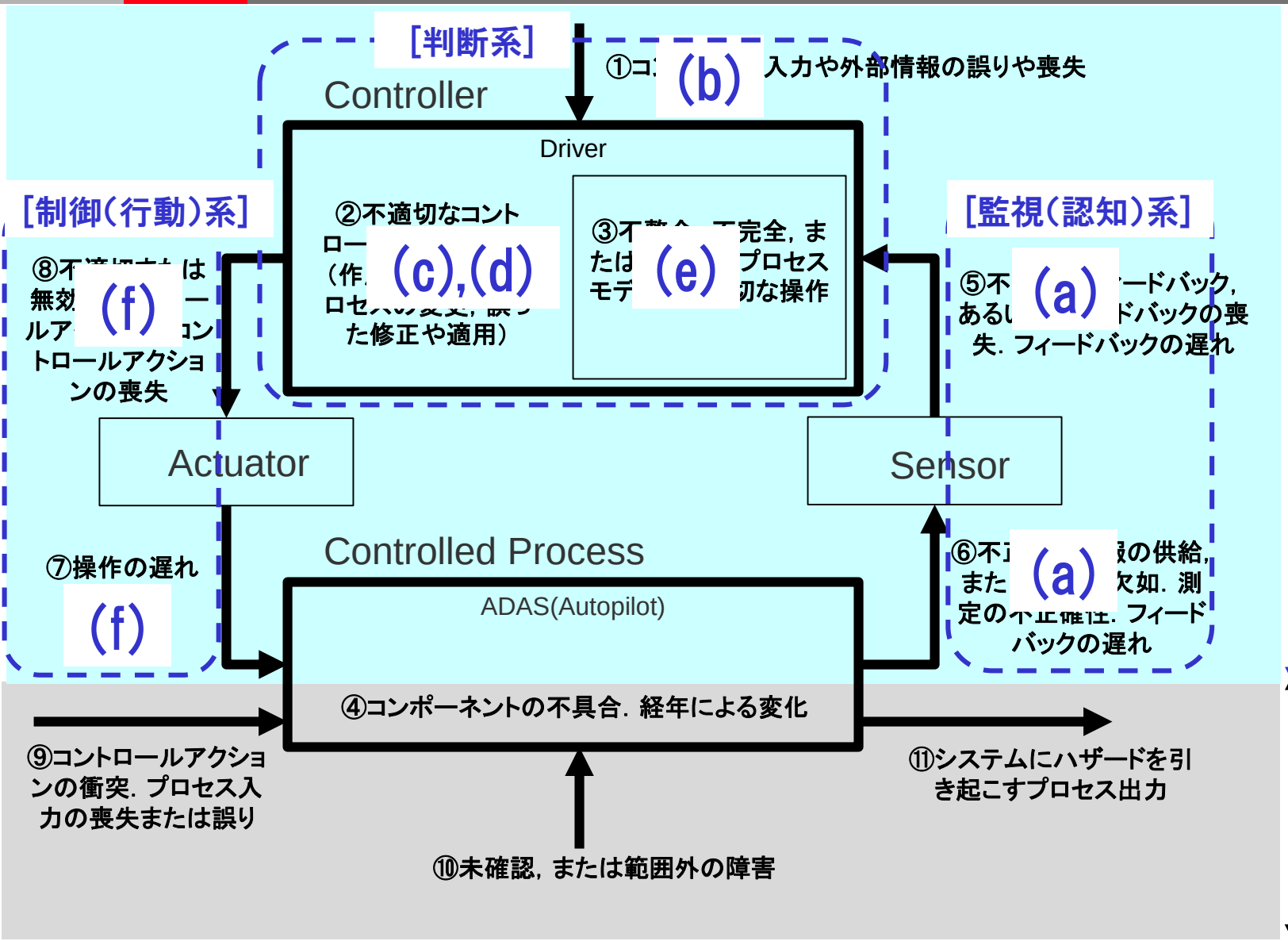
- 自動化システム使用継続で技量の低下

[制御(行動)系]

(f)無理な要求によるヒューマンエラー誘発

- 多機能・多様HMI、緊急時等手動切替で高すぎるワークロード

3-4. CFコントロールループ図上への自動化HFの対応づけ



3-5. ADAS/MMI分析向け要因CF抽出のガイドワード一覧

HITACHI
Inspire the Next

＜STPA標準ガイドワード＞

① [xxx]コントロール入力や[xxx]外部情報の誤りや喪失.
② 不適切な[xxx]コントロールアルゴリズム(作成時の欠陥, プロセスの変更, 誤った修正や適用).
③ 不整合, 不完全, または不正確な[xxx]プロセスモデル. 不適切な操作.
④ [xxx]コンポーネントの不具合. 経年による変化.
⑤ [xxx]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. フィードバックの遅れ.
⑥ [xxx]不正確な情報の供給, または情報の欠如. 測定の不正確性. フィードバックの遅れ.
⑦ [xxx]操作の遅れ.
⑧ [xxx]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の喪失.
⑨ [xxx]コントロールアクションの衝突. プロセス入力の喪失または誤り.
⑩ [xxx]未確認, または範囲外の障害.
⑪ [xxx]システムにハザードを引き起こすプロセス出力.

[xxx]:割付・具体化、yyy:詳細化

＜ADAS/MMI向け特化ガイドワード＞

① [ドライバーの]運転介入削減による退屈感や[メーカ]の自動運転仕様提示の誤りやそれらによる危機感の喪失.
② 不適切な[ADASの]操作手順(過信・不信による自動運転の誤った使用).
③ 不整合、不完全、または不正確な[ADAS⇔ドライバー]SVC役割分担プロセスモデル. 技量低下・欠如による不測事態の不適切な操作.
④ [ADAS]コンポーネントの不具合、経年による変化.
⑤ [ドライバーへの]不適切な運転状況認識情報の通知、あるいは運転状況認識情報通知の喪失、運転状況認識情報通知の遅れ.
⑥ [ADASからの]不正確な運転状況認識情報の供給、または運転状況認識情報の欠如、測定の不正確性、運転状況認識情報通知の遅れ.
⑦ [ADASへの]無理な要求による操作の遅れ.
⑧ [ドライバーからの]無理な要求下による不適切または無効な運転操作、運転操作の喪失.
⑨ [自動車]制動との衝突、操舵入力の喪失または誤り.
⑩ [運転環境からの]未確認、または範囲外の障害.
⑪ [ADASからの]自動車にハザードを引き起こすプロセス出力.

赤色:自動化HF反映特化、青色:標準対象特化

3-6. 適用例;参考元_2016/5_T社モデルXの事故・対応概要

HITACHI
Inspire the Next

事故概要;[自動運転初の死亡事故]
“左折しようとしたトレーラが4車線の国道上を直角に横切っていたところへ、
モデルXが直進してきて衝突、モデルXドライバーが死亡した事故”
(事故主原因;優先権があったモデルXに道を譲らなかったトラック運転手の過失)

＜当時挙げれていたモデルX側原因群＞

- 前方衝突を避けるために作動する自動ブレーキ/アラート機能が作動せず
  - トレーラ側面の光加減・色・車高の高さで、センサー(カメラ)が、トレーラを検知不能
  - 製造メーカによれば、搭載のレーダーは、前方追突防止の機能であり、横から出てくる車との衝突回避不能
- レベル2ADASの運転支援システムを「オートパイロット」と誇張・過信?(車内でDVD鑑賞?)
- ドライバーが4分以上ハンドルから手を離すことが可能(他社は不可:15秒程度)

＜モデルXの再発防止策＞

■ ADASソフトのバージョンアップ

- 周囲検知には、カメラよりもレーダーを重視し、周辺前方向に対して3D物体検知
- ハンドルから手を離した場合のドライバーへのアラート機能及び無視した場合のオーパイモード解除機能

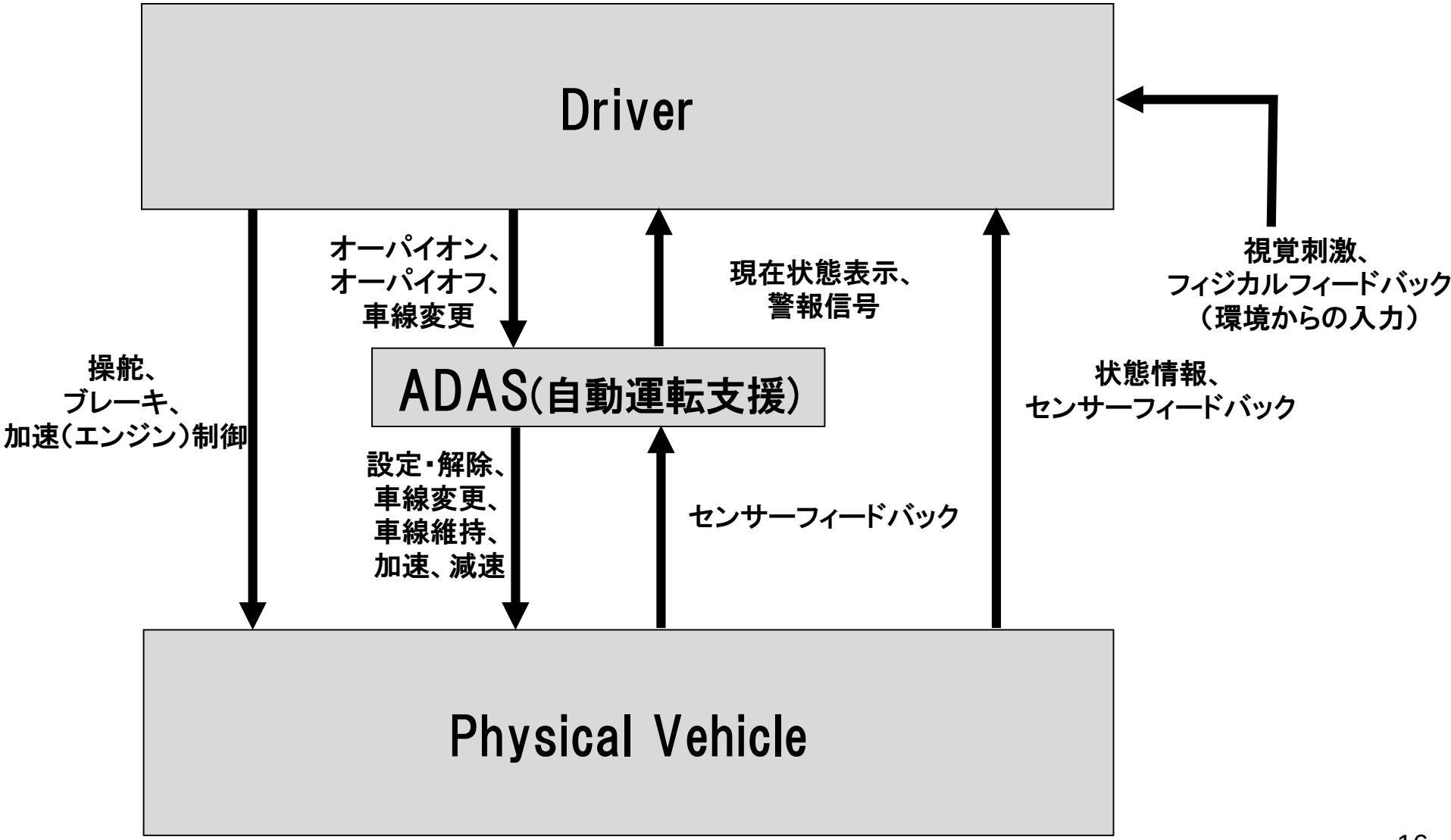
対応十分?
(機械側の改善・強化中心で良いのか?)

参考;http://www.shippai.org/shippai/html/index.php?name=news905

3-7. 適用例；自動運転（SVC）系の セーフティコントロールストラクチャ

HITACHI
Inspire the Next

- 対象事故；自車と他車両との衝突死亡事故
- 対象ハザード；センサー攻撃による近傍車両との安全車間距離維持不能



3-8. 適用例；自動運転（SVC）系のUCAの識別

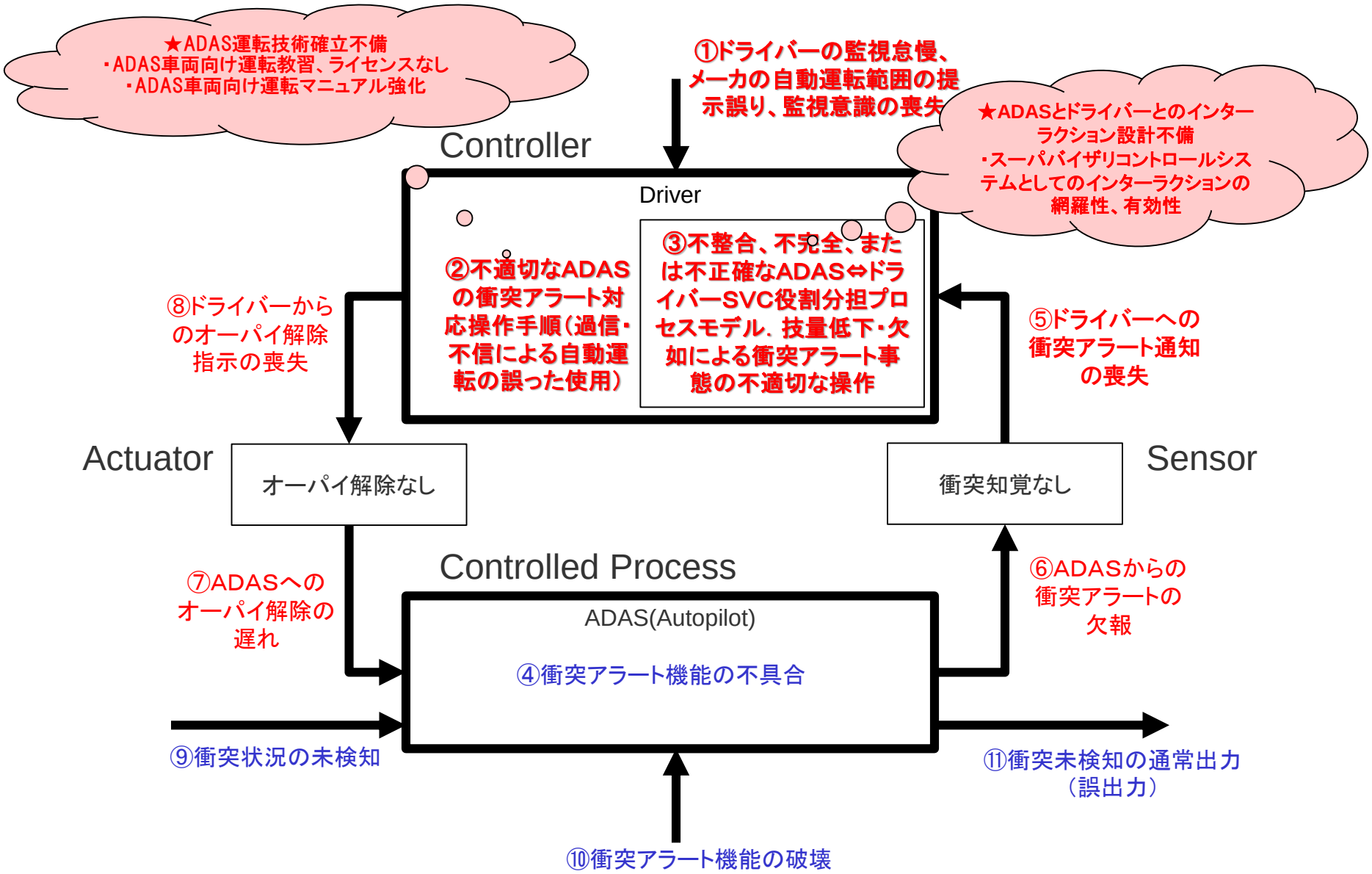
HITACHI
Inspire the Next

IFポイント	From ⇒To	Control Action / Feed Back	Not providing	Unsafe control action	Too early, too late, out of sequence	Stopping too soon or continuing too long
Physical Vehicle⇔ADAS（M⇔Mインターラクション）	Physical Vehicle ⇒ADAS	センサー情報の通知	非通知	誤報通知	通知遅延	通知停止
	ADAS⇒ Physical Vehicle	速度減速指示	指示未伝達	誤指示伝達	指示伝達遅延	指示伝達不良（停止・長時間継続）
ADAS⇔Driver（M⇔Hインターラクション）	ADAS⇒ Driver	アラート通知	非通知	誤報通知	通知遅延	通知停止
	Driver⇒ ADAS	オーバイ解除指示	指示未伝達	誤指示伝達	指示伝達遅延	指示伝達不良（停止・長時間継続）
Environment⇔Driver（E⇔Hインターラクション）	Environment⇒Driver	視覚的行動サイン	視覚的監視不能	視覚的監視不備（運転違反・条件非順守）	視覚的監視遅延	視覚的監視停止

以降、詳細分析

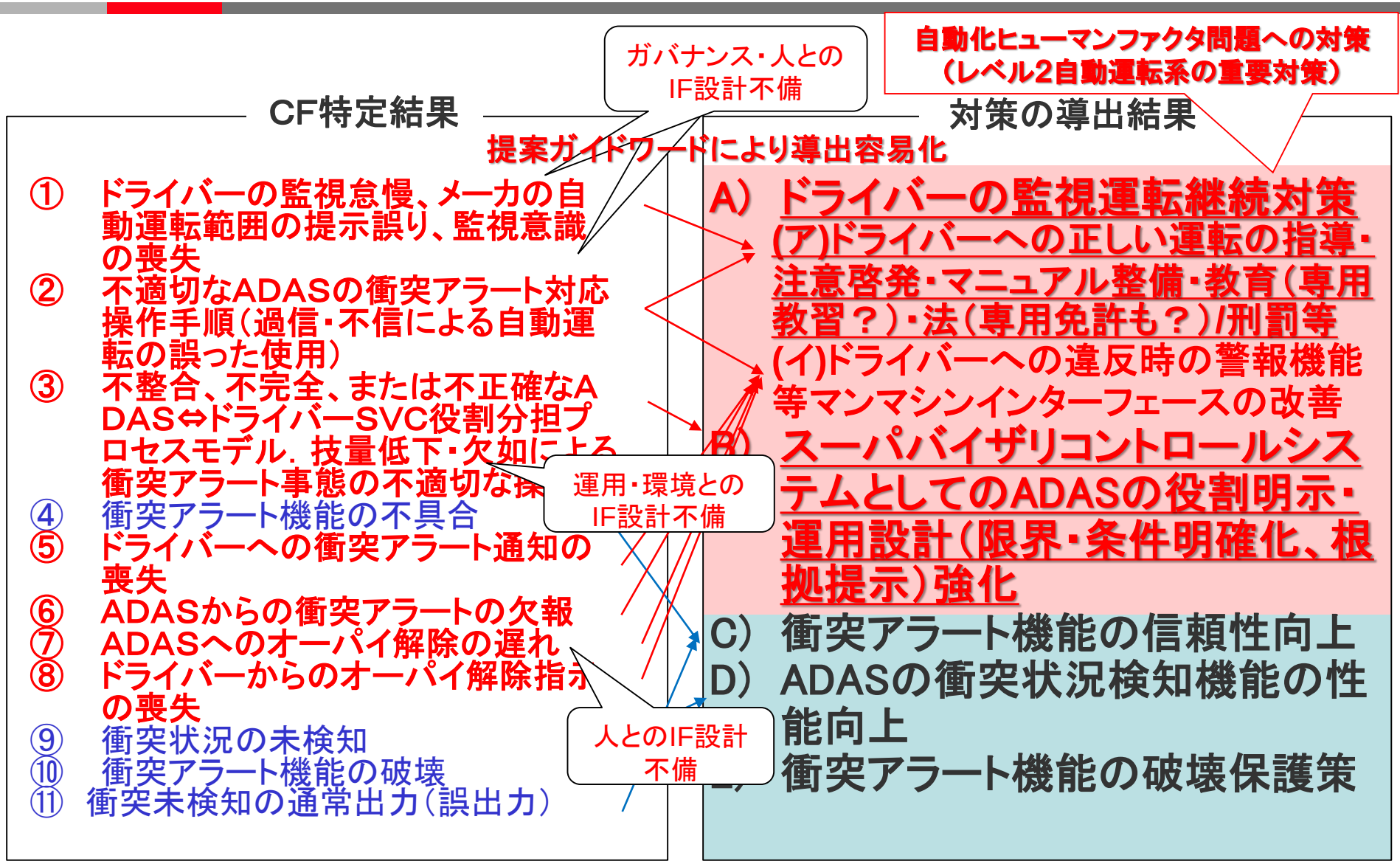
3-9. 適用例；UCA“衝突アラートの非通知”の提案ガイドワードによるCF導出のコントロールループ図

HITACHI
Inspire the Next



3-10. 適用例；UCA“衝突アラートの非通知”の提案ガイドワードによるCF特定結果と対策の導出結果

HITACHI
Inspire the Next



従来ガイドワードでも導出可能範囲

3-11. 適用例；STPA特徴導出対策とT社再発防止策との比較評価
（　レベル2・3自動運転系の重要課題　）

HITACHI
Inspire the Next

対策の導出結果

現状のT社再発防止策等

提案ガイドワードによる導出対策と再発防止策との対応

A）ドライバーの監視運転継続対策
(ア)ドライバーへの正しい運転の指導・注意啓発・マニュアル整備・教育（専用教習？）・法（専用免許も？）/刑罰等
(イ)ドライバーへの違反時の警報機能

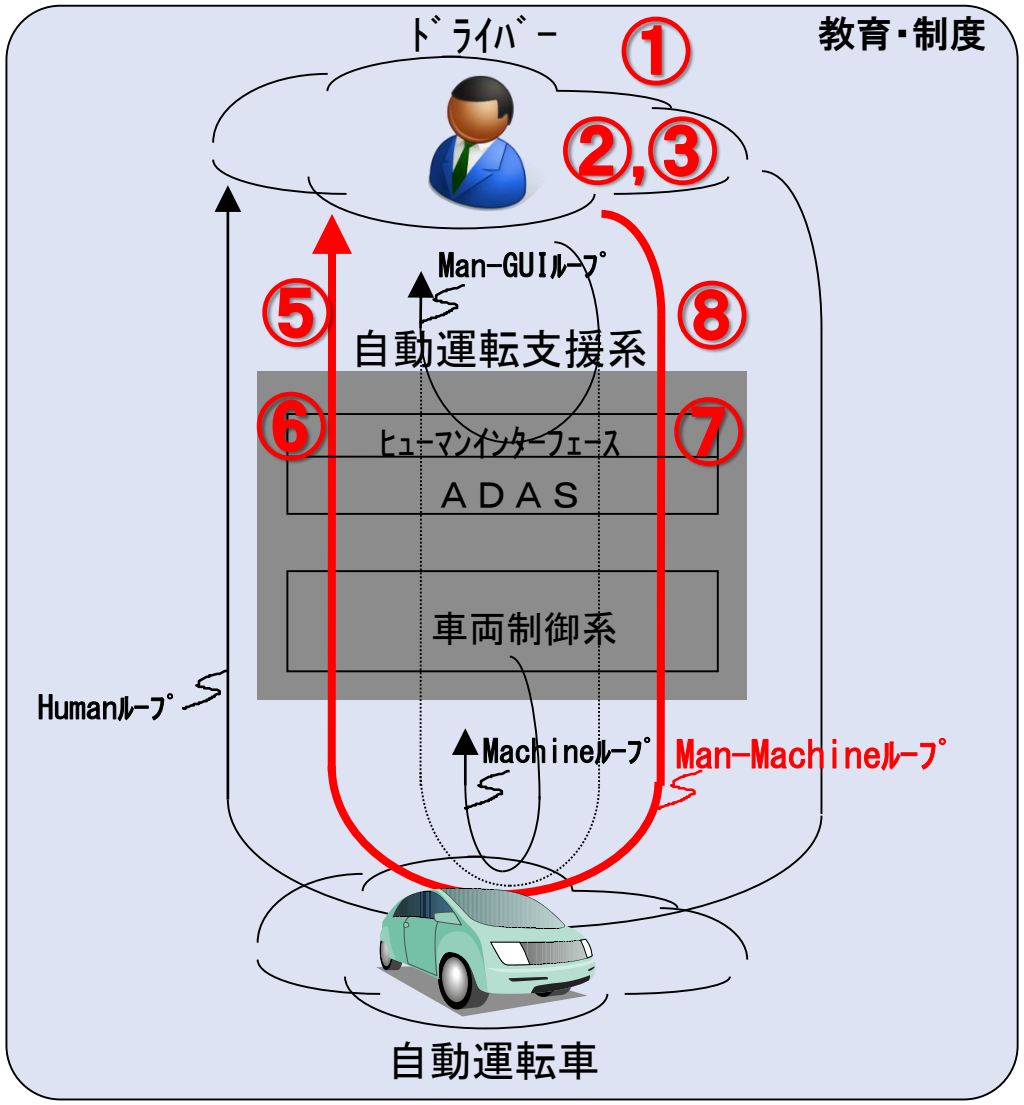
B）スーパバイザリコントロールシステムとしてのADASの役割明示・運用設計（限界・条件明確化、根拠提示）強化

- T社；ADASソフトのバージョンアップによる機能追加・改善
  - ハンドルから手を離した場合のドライバーへのアラート機能及び無視した場合のオーバイモード解除機能

☆⇒対応不十分？
・ADASドライバーのモラル・教習
・ADAS自動運転車に関する法整備
（規制・罰則、免許制度等）

☆⇒対応不十分？
・スーパバイザリコントロールシステムとしての明示的・体系的運用安全設計
（運転モードで動的・適応的機能配分、自動運転レベル・モード・根拠情報の表示等HMI強化、オーナーマニュアル記載等）
（ドライバー視点で、できる事とできない事、利用条件・範囲明示等）

3-12. 適用例；提案ガイドワードの有効性



シェリダンのマン・マシンシステムの対話ループモデル

＜提案ガイドワードだから抽出できた異常＞

① ドライバーの監視怠慢（メーカ手離し許可？）、メーカの自動運転範囲の提示誤り、監視意識の喪失
② 不適切なADASの衝突アラート対応操作手順（過信・不信による自動運転の誤った使用）
③ 不整合、不完全、または不正確なADAS⇔ドライバーSVC役割分担プロセスモデル．技量低下・欠如による衝突アラート事態の不適切な操作
⑤ ドライバーへの衝突アラート通知の喪失
⑥ ADASからの衝突アラートの欠報
⑦ ADASへのオーバイ解除の遅れ
⑧ ドライバーからのオーバイ解除指示の喪失

SVCのMan-Machineループ関連の不備を容易に抽出

従来（手動運転支援）の延長でなく、Man-Machineループ（監視制御系）の観点からの対策見直し・整備要
⇒人と知的システムとのインターラクション解析に有効！

M:Machineループ（情報システム機能で自動的に達成される処理）
M-M:Man-Machineループ（人間が情報システム機能を利用して達成する処理）
M-G:Man-GUIループ（人間と情報システムＧＵＩ間で達成される処理）
H:Human(Man)ループ（人間の能力のみで達成する処理）

4. まとめ(提案内容と適用例、今後の課題)

HITACHI
Inspire the Next

◆ 提案内容
- STAMP/STPAを利用した自動化システム⇔人間間のヒューマンファクタ問題のCFを体系的、容易に導出するために、
  - CFガイドワードのクラス階層構造化定義と、
  - 先行航空分野の知見反映による自動化ヒューマンファクタ向けガイドワードを提案
- 適用例で自動化ヒューマンファクタCFを体系的に抽出可能であることを確認
  - ガバナンス(管理・教育)観点;
    - ✓ ADAS性能の過信・誤解(OEMの誇張影響も)
      - 正確な性能範囲の啓発・周知・教育の必要
    - ✓ ADAS自動運転車に関する法整備(規制・罰則、免許、保険)
      - レベル2向け対応(レベル2教習・免許等)
  - SVCシステム観点;
    - ✓ 体系的ADAS運用設計の不備(レベル2の体系的運用設計;できる事とできない事、利用条件・範囲等)
      - SVCシステム向け運用設計強化(監視制御系の強化)

◆ 今後の課題
- 自動運転系適用評価・有効性検証の拡充
- 自動化ヒューマンファクタガイドワードの洗練・拡充
- 他自動化(AI利用等)分野のMMIへの適用評価・検証

HITACHI
Inspire the Next

END

自動運転系の安全・セキュリティ解析のための自動化ヒューマンファクタに基づくSTPAガイドワードの提案

2017/11/28

株式会社　日立製作所　サービスプラットフォーム事業本部
セキュリティ事業統括本部

永井康彦