2018年12月4日
第3回 STAMPワークショップ

STAMP/STPAを用いた自動運転車両の安全解析
～操舵系に関するミスユース～

・JARI第31研究室　株式会社ジェイテクト
研究開発本部　システム創生研究部
森木　紘平（発表者）
・一般社団法人　日本自動車研究所
ITS研究部

発表内容

1．背景および目的

2．ミスユース安全設計

3．STAMP/STPAによる分析

4．課題に対する取組み

5．まとめ

会社紹介

■会社名

株式会社ジェイテクト（2006年1月に光洋精工と豊田工機が合併）

■本店、本社所在地

名古屋本社　名古屋市中村区名駅4丁目7番1号　ミッドランドスクエア15階
大阪本社(本店)　大阪市中央区南船場3丁目5番8号

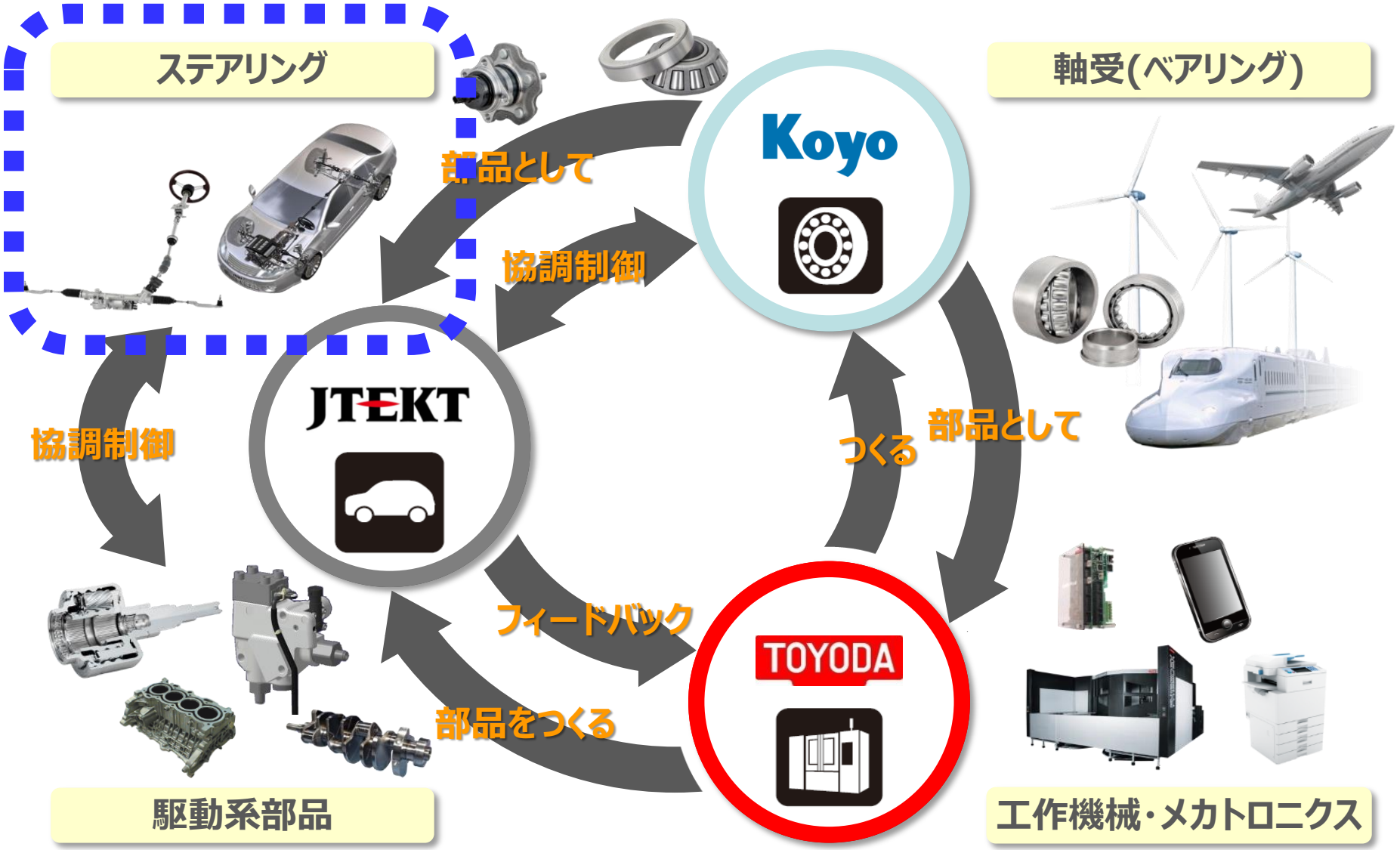
■資本金、売上高、従業員数

資本金　：45,591　百万円　(平成30年3月現在)
売上高　：連結：　1,441,170　百万円、単独：　647,101　百万円　(平成30年3月期)
従業員数：連結：　49,589名、単独：　11,763名　(平成30年3月現在)

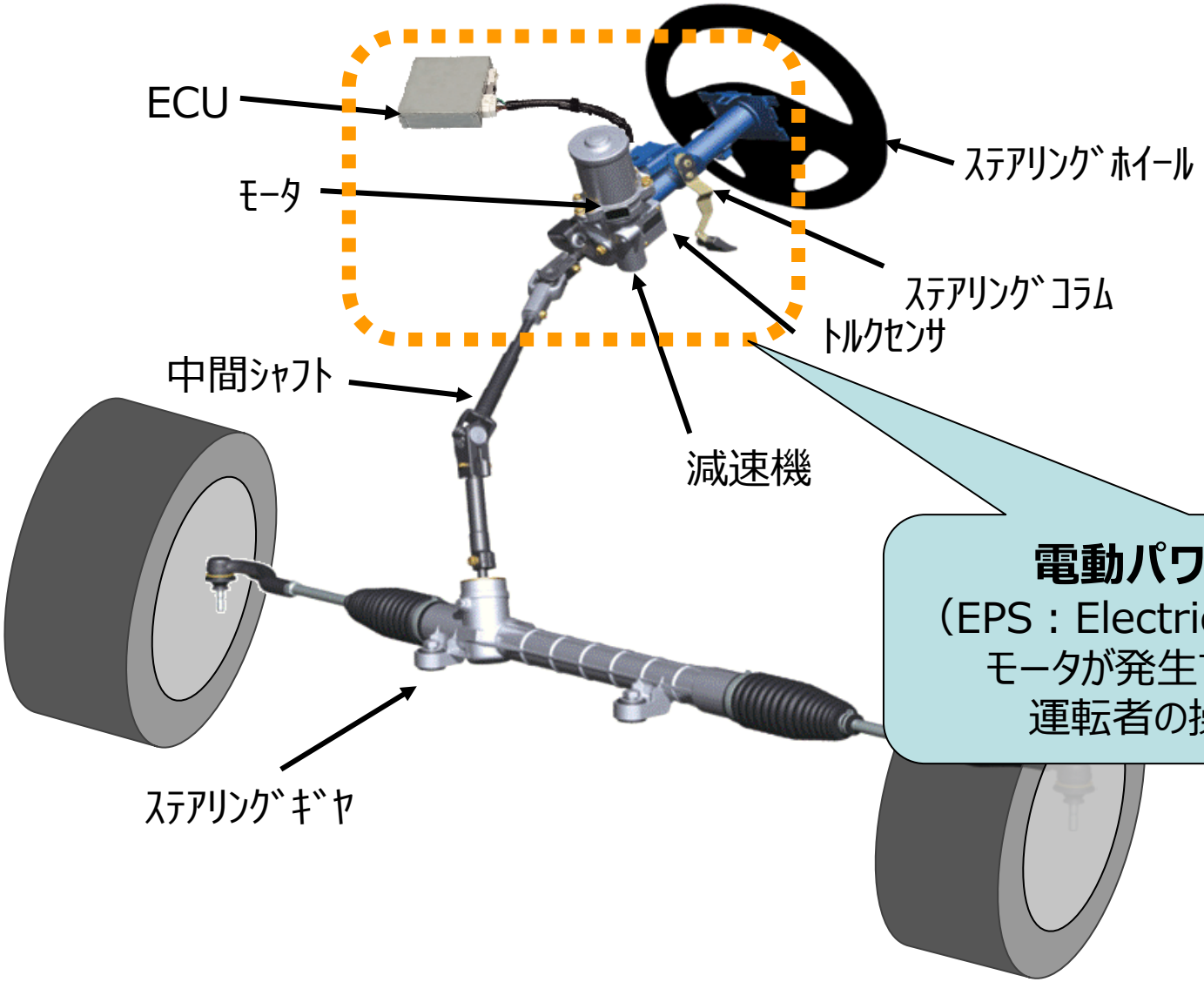
■トヨタグループ

・トヨタ自動車株式会社
・株式会社豊田自動織機
・愛知製鋼株式会社
・株式会社ジェイテクト
・トヨタ車体株式会社
・豊田通商株式会社
・アイシン精機株式会社
・株式会社デンソー
・トヨタ紡織株式会社
・東和不動産株式会社
・株式会社豊田中央研究所
・トヨタ自動車東日本株式会社
・豊田合成株式会社
・日野自動車株式会社
・ダイハツ工業株式会社
・トヨタホーム株式会社
・トヨタ自動車九州株式会社

会社紹介


ステアリング
軸受(ベアリング)
部品として
協調制御
Koyo
協調制御
JTEKT
つくる
部品として
フィードバック
TOYODA
部品をつくる
駆動系部品
工作機械・メカトロニクス

電動パワーステアリング紹介

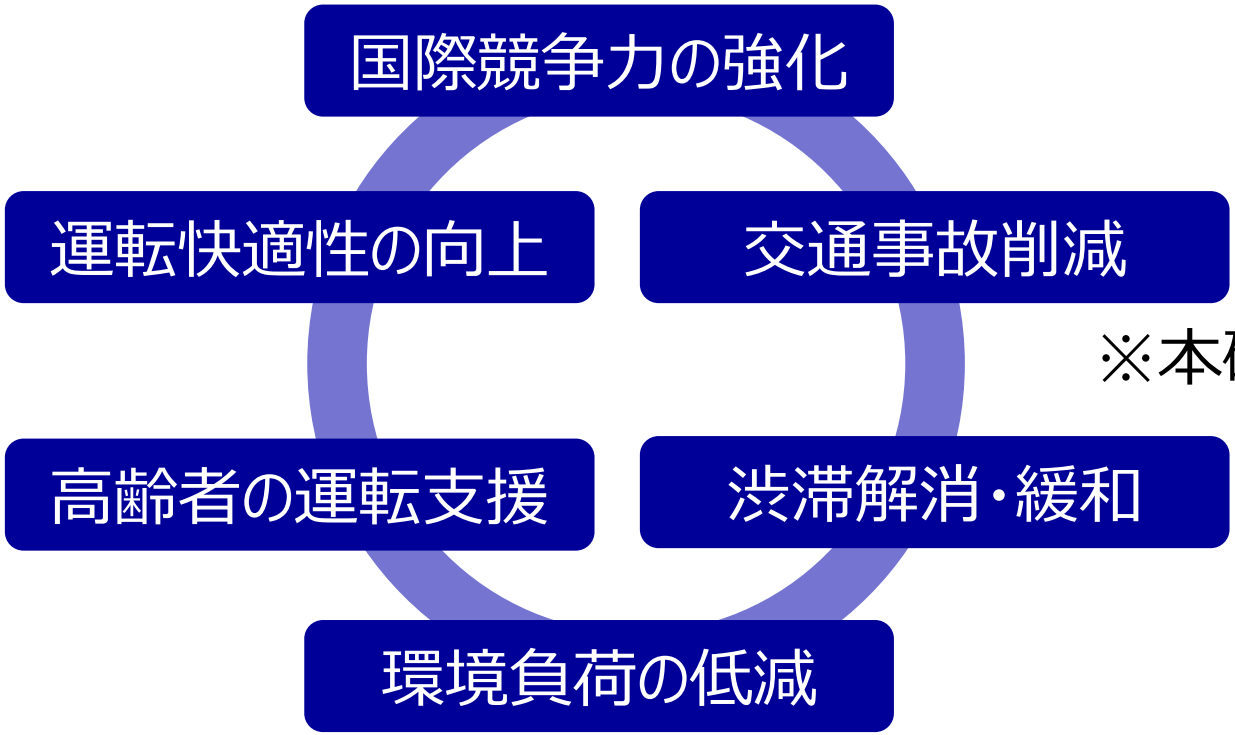


電動パワーステアリング
（EPS：Electric Power Steering）
モータが発生する回転力によって
運転者の操舵力をアシスト

研究背景

■ 自動運転社会の実現に向け 国内外問わず 開発が進む

自動運転社会の実現による主な効果



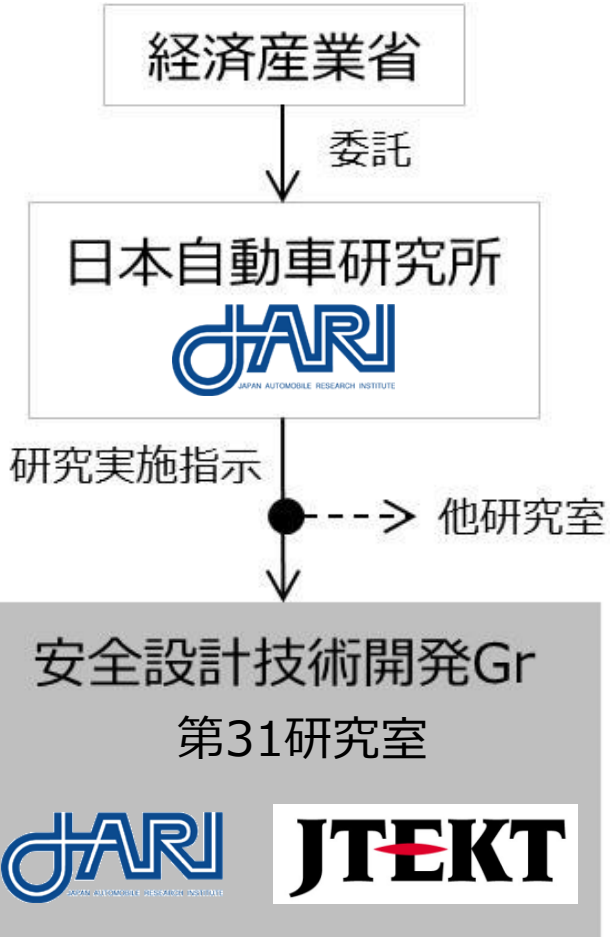
※本研究背景

引用元：平成25年度 国交省「オートパイロットシステムの実現に向けて」中間とりまとめ案

研究実施体系

【高度な自動走行システムの社会実装に向けた研究開発・実証事業】

テーマ名：セーフティ・セキュリティ技術評価環境の構築



・JARI研究室として参画
・平成26年度から5ヵ年
・協調領域の取り組み

※「JARI」は　一般財団法人日本自動車研究所の商標登録である

研究対象

【高度な自動走行システムの社会実装に向けた研究開発・実証事業】

テーマ名：セーフティ・セキュリティ技術評価環境の構築

■ 交通事故を削減 ＝ 自動運転に起因する事故リスク減

■ 想定される自動運転に起因する事故原因（例）

➢自動運転システムの故障

・要求された機能を実行するエレメントの能力の停止

➢自動運転システムの性能限界

・設計時に想定する作動範囲を外れたり、外乱等で意図した性能が発揮できない状態

➢ドライバの誤使用・誤操作

・設計者が本来意図している使い方と異なった、使用者による不適切な使用（誤使用）

・使用者には設計者が意図した通りに使う意思があるが、操作を誤る（誤操作）

自動運転の課題とレベル定義

【高度な自動走行システムの社会実装に向けた研究開発・実証事業】

テーマ名：セーフティ・セキュリティ技術評価環境の構築

■ ドライバの誤使用・誤操作に対する課題

システムに故障が無くても誤使用・誤操作により非安全な状態に陥る可能性がある

■ 自動運転のレベル定義

：システム主体

SAE レベル	SAE 名称	操作の 実行主体	走行環境 監視	バックアップ (緊急時)	システム 能力
0	非自動化	ドライバ	ドライバ	ドライバ	制限あり
1					
2	一部自動化		ドライバ	ドライバ	制限あり
3	条件付自動化	システム	システム	ドライバ	制限あり
4	高度自動化	システム	システム	システム	制限あり
5	完全自動化	システム	システム	システム	制限なし

ドライバの誤使用・誤操作が発生する可能性がある

SAE： Society of Automotive Engineers

研究目的と目標

【高度な自動走行システムの社会実装に向けた研究開発・実証事業】

テーマ名：セーフティ・セキュリティ技術評価環境の構築

■ 目的

- 自動運転システム(SAEレベル3)において、非安全な状態を引き起こしかねない、ミスユース（誤使用・誤操作）を考慮することが必要
- 操舵制御系を例題に、ミスユース課題に対する安全設計方法、および、検証・評価方法（プロセス含）の事例を提示

■ 目標

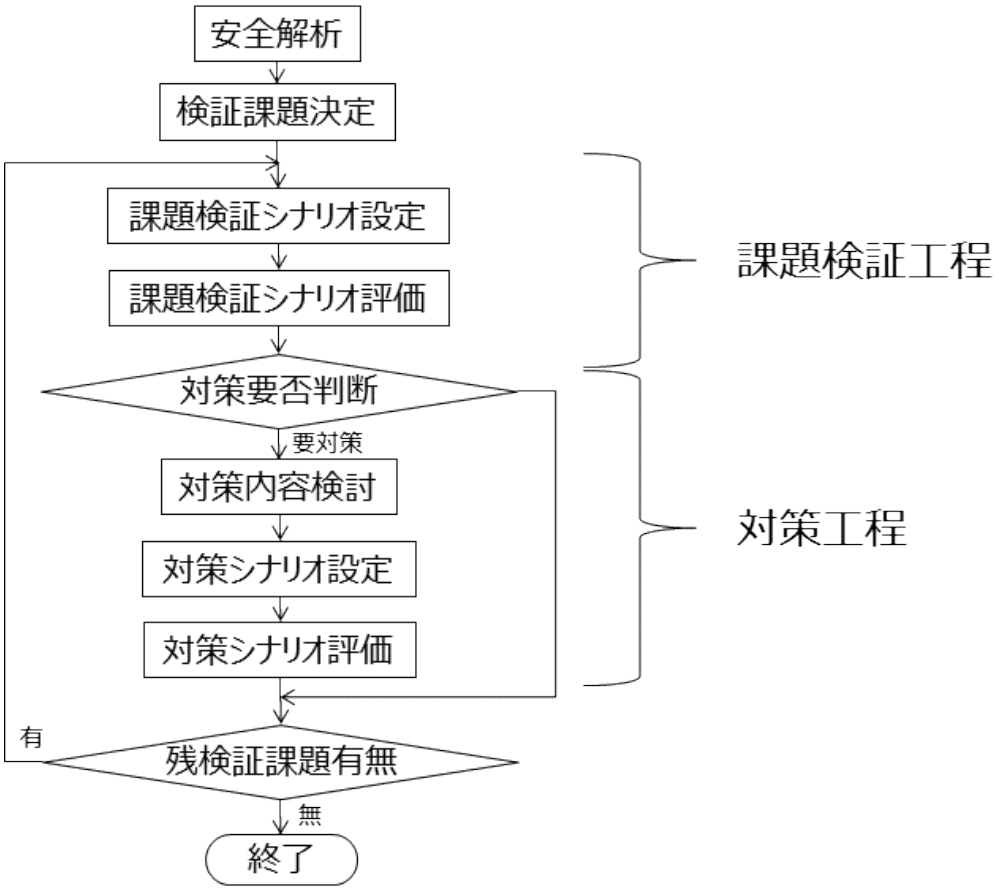
- 得られた成果(安全設計／検証評価の考え方・方法事例)を、「個社開発」「実証事業」などのバックデータとして活用頂く

目標に対する提案内容

【高度な自動走行システムの社会実装に向けた研究開発・実証事業】

テーマ名：セーフティ・セキュリティ技術評価環境の構築

■ ミスユース安全設計検討プロセス



研究実施計画

【高度な自動走行システムの社会実装に向けた研究開発・実証事業】

テーマ名：セーフティ・セキュリティ技術評価環境の構築

平成29年度までの公開内容：自動運転の安全設計や課題、検証方法

注）本研究の成果は、平成28～29年度の経済産業省委託業務「高度な自動走行システムの社会実装に向けた研究開発・実証事業」で得られたものである

発表内容

1．背景および目的

2．ミスユース安全設計

3．STAMP/STPAによる分析

4．課題に対する取組み

5．まとめ

ミスユース安全設計

ミスユースの定義

誤使用・誤操作を「ミスユース」と総称する

誤使用　：設計者が本来意図／推奨している使い方と異なった、
使用者による不適切な使用のこと。※

本事業では「悪意をもった使用」も含んだ意味と捉える。

誤操作　：使用者には設計者が意図した通りに使用する
意思があるが、結果として操作を誤ること。※

※引用元　：自動走行ビジネス検討会公開資料
「自動走行ビジネス検討会　今後の取組方針」

ミスユース安全設計

自動運転レベル別詳細内容

システムによる監視

ドライバーによる監視

高速道路での完全自動運転
（2025年目途）

レベル5

○完全自動運転
常にシステムが全ての運転タスクを実施

限定地域での無人自動運転移動サービス（2020年まで）

レベル4

○特定条件下における完全自動運転
特定条件下においてシステムが全ての運転タスクを実施

*6

高速道路等一定条件下での自動運転モード機能を有する「自動パイロット」
（2020年目途）

レベル3

○条件付自動運転
システムが全ての運転タスクを実施するが、システムの介入要求等に対してドライバーが適切に対応することが必要

*5

○特定条件下での自動運転機能（高機能化）
【例】 高速道路での自動運転モード機能
①遅いクルマがいれば自動で追い越す
②高速道路の分合流を自動で行う

*4

レベル2

○特定条件下での自動運転機能（レベル1の組み合わせ）
【例】車線を維持しながら前のクルマに付いて走る（LKAS+ACC）

○運転支援　システムが前後・左右のいずれかの車両制御を実施

【例】自動で止まる
（自動ブレーキ）

*1

前のクルマに付いて走る
（ACC）

*2

車線からはみ出さない
（LKAS）

*3

レベル1

ACC：Adaptive Cruise Control，LKAS：Lane Keep Assist System

引用元：国土交通省HP

ミスユース安全設計

想定する自動運転車両

SAE レベル	SAE 名称	操作の 実行主体	走行環境 監視	バックアップ (緊急時)	システム 能力
3	条件付自動化	システム	システム	ドライバ	制限あり
4	高度自動化	システム	システム	システム	制限あり
5	完全自動化	システム	システム	システム	制限なし

自動運転レベル3

一般的な乗用車

オーバーライドによる権限委譲可能

TOR

音声

表示

応答

押し ボタン

声

TOR(Take Over Request)で権限委譲依頼を受け運転者が応答

ミスユース安全設計

日本での自動車業界と航空機業界との免許制度の比較

	自動車運転者	航空機操縦士
操縦可能機種数	無制限	機種毎
免許更新	・5年or3年 ・講習 ・視力検査	・半年（機長） ・実技試験 ・身体検査
免許保有数	82,000,000人（H29 年）	5,686人（H25年）

自動運転でミスユースの発生する可能性

自動車運転者 ＞ 航空機操縦士

ミスユース安全設計

航空機業界における自動操縦でのミスユース事故事例

	エアバス社	ボーイング社
自動操縦設計思想	システム優先	人間優先
	自動操舵中、機体傾き安全範囲を超える操縦は全てキャンセルされる。 ※安全範囲内は制御可能	機体傾き安全範囲を超える操縦は桿が重くなる事で抑止させる。更に強い力で押し込むと、その行為が必要だと判断し主権を人間に与え安全範囲を超えて機体が傾く。
自動操縦解除方法	ボタン＋操縦桿操作（A320以降） ※以前は所定のシーケンス要	操縦桿操作
事故事例	・自動操縦の解除ができず手動操縦と干渉が発生 ・パイロットが自身の子どもを操縦席に座らせていたところ、自動操縦解除させた事に気づかなかった	・誤って操縦桿を動かした事に気づかず自動操縦が継続していると思い込んだ

ミスユース安全設計

自動運転車で想定するミスユース（一例）

ミスユースを安全解析する必要がある

ミスユース安全設計

自動運転車両のミスユースの安全解析への対応

■ 安全解析での懸念点

①ミスユースはシステムが故障していないため、従来の故障解析を適用しにくいのではないか

②自動運転車両と人間とのやり取りであり、システムが複雑となっていて、システムを把握できないのではないか

■ STPAの利点

・システムの構成要素が故障していなくても、構成要素間の非安全な相互作用による事故の安全解析ができる

・非常に複雑なシステムを安全解析することができる

STAMP/STPAによる安全分析手法を選択

発表内容

1．背景および目的

2．ミスユース安全設計

3．**STAMP/STPAによる分析**

4．課題に対する取組み

5．まとめ

STAMP/STPAによる分析

Step0

- システムにおけるミスユース対象範囲の明確化
  - アクシデント、ハザード、安全制約の定義
  - コントロールストラクチャの構築とコントロール仕様の定義

Step1

- ミスユースに関連する非安全シナリオの抽出

Step2

- 非安全シナリオに対するハザード要因の抽出

STAMP/STPAによる分析

前提条件

SAE レベル	SAE 名称	操作の 実行主体	走行環境 監視	バックアップ (緊急時)	システム 能力
3	条件付自動化	システム	システム	ドライバ	制限あり
4	高度自動化	システム	システム	システム	制限あり
5	完全自動化	システム	システム	システム	制限なし

自動運転レベル3

一般的な乗用車

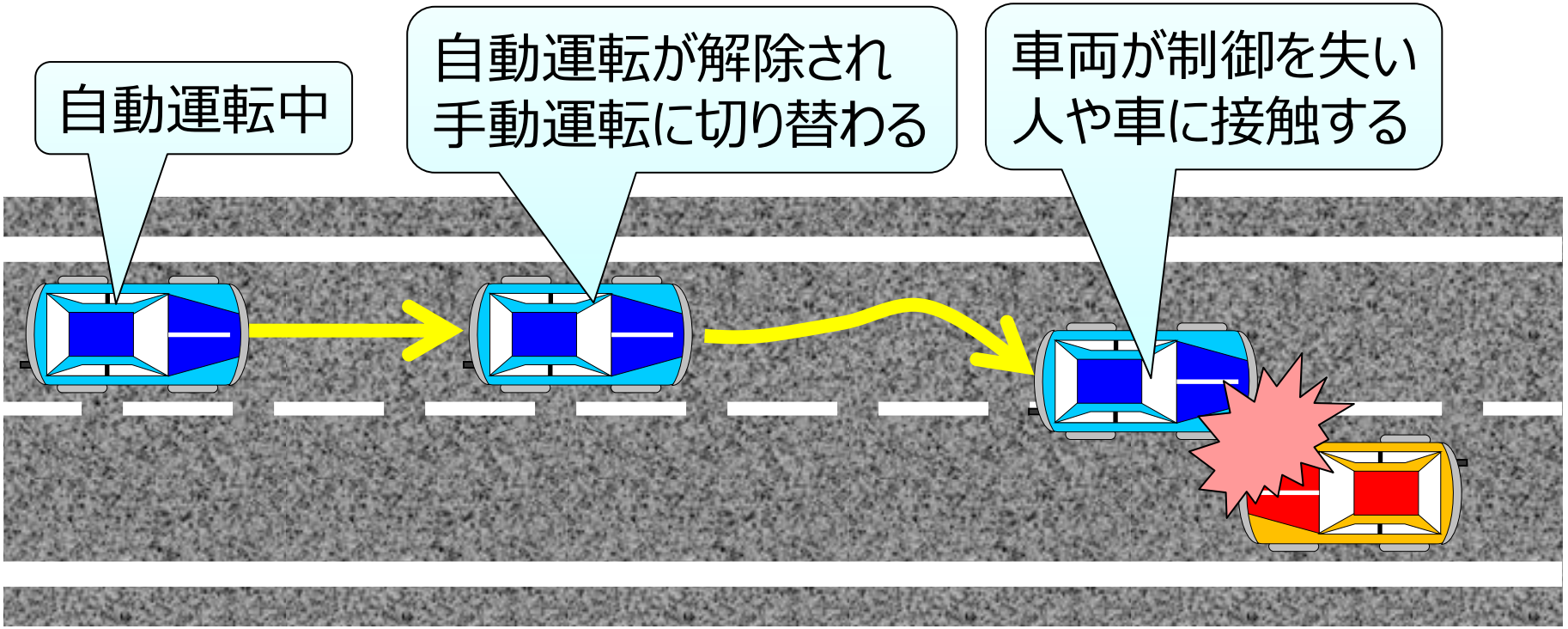
オーバーライドによる権限委譲可能

TOR(Take Over Request)で権限委譲依頼を受け運転者が応答

STAMP/STPAによる分析

アクシデント、ハザード、安全制約の識別（STEP0-1）

●想定するアクシデントの一例



手動運転に切り替わったことをドライバが気づいていなければ・・・

STAMP/STPAによる分析

アクシデント、ハザード、安全制約の識別（STEP0-1）

アクシデント	ハザード	安全制約
自動運転車両が人・車と衝突する	運転者の意図なしに自動運転モードが切り替わる（第三者の悪意による切り替えを含む）	運転者が意図しない状況では自動運転モードを切り替えない
	車両の正しい自動運転モードが正しいタイミングで運転者に伝わらず、運転者が車両状態と異なる運転操作を行う　（または、必要な運転操作を行わない）	運転者が十分追従できるタイミングで意図する自動運転モードに切り替える、もしくは運転者の意図（操作）と車両状態の不一致がある場合は運転者に気づかせる
	システムが自動運転解除を必要とする時に、運転者が自動運転解除を認識しない（悪意を含む）	自動運転解除要求を運転者に確実に認知させる

※自動運転システムが正常に作動している時は事故に至らない
※不具合や性能限界に起因するアクシデントは分析の対象外
※安全性に関わらない事象は対象外

STAMP/STPAによる分析

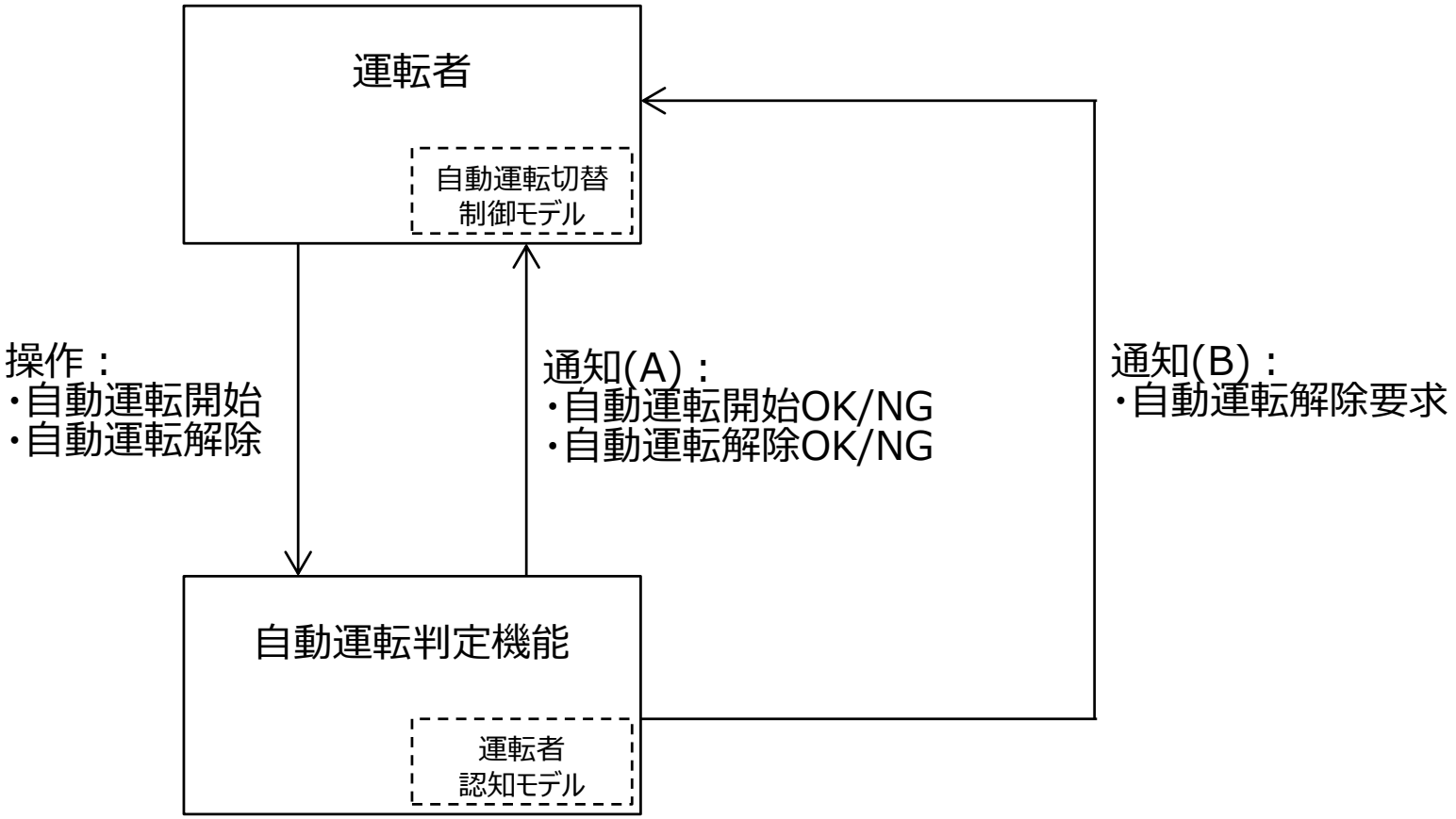
コントロールストラクチャの構築（STEP0-2）

●ミスユースが発生すると想定するシステム

ステアリング（操舵系）を含むシステムで検討を行う。

STAMP/STPAによる分析

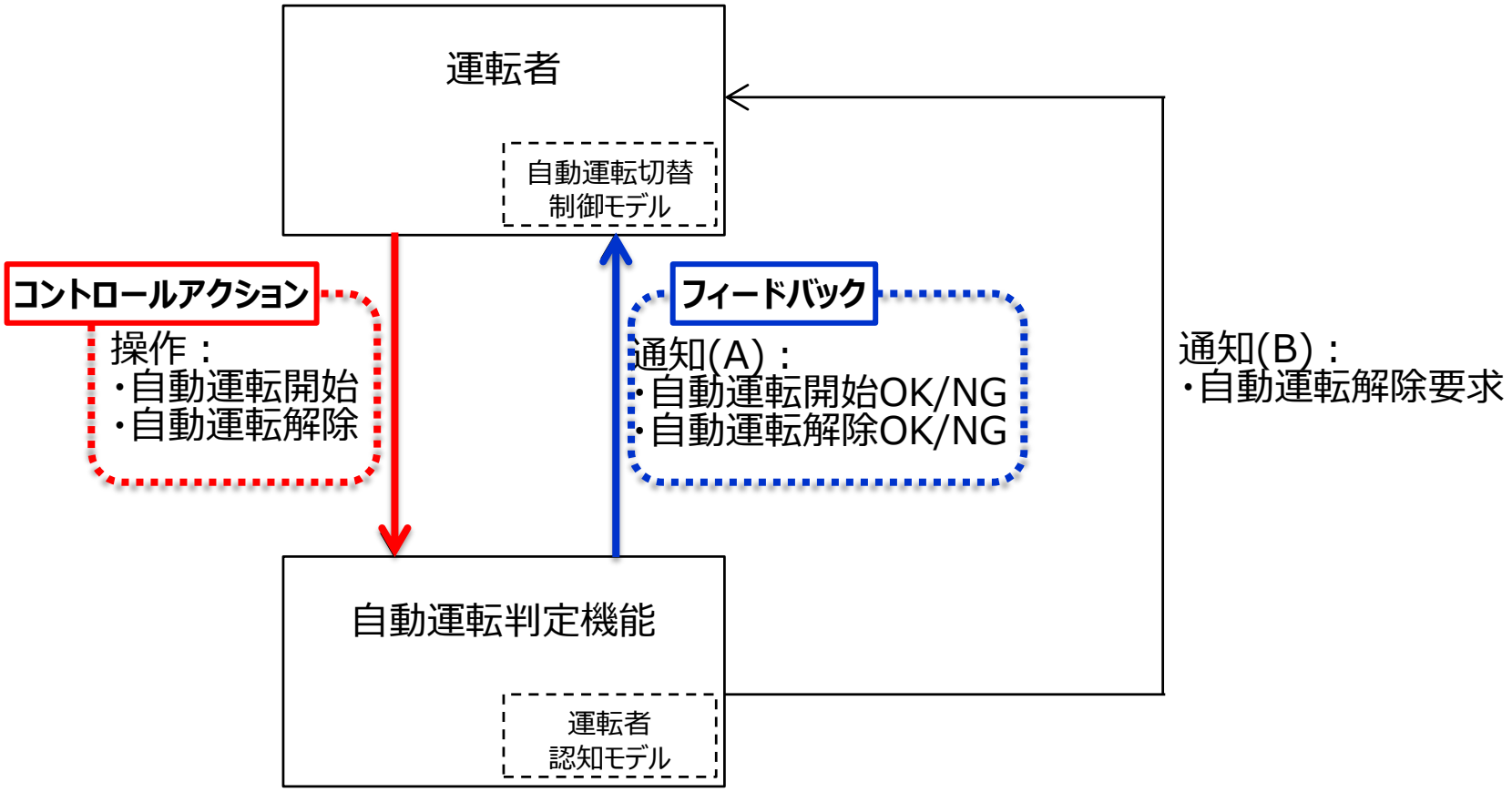
コントロールストラクチャの構築（STEP0-2）



※情報伝達手段は限定せず、視覚・聴覚・触覚による情報伝達全般を対象
※網羅的な検証とするため、詳細な仕様策定はしない

STAMP/STPAによる分析

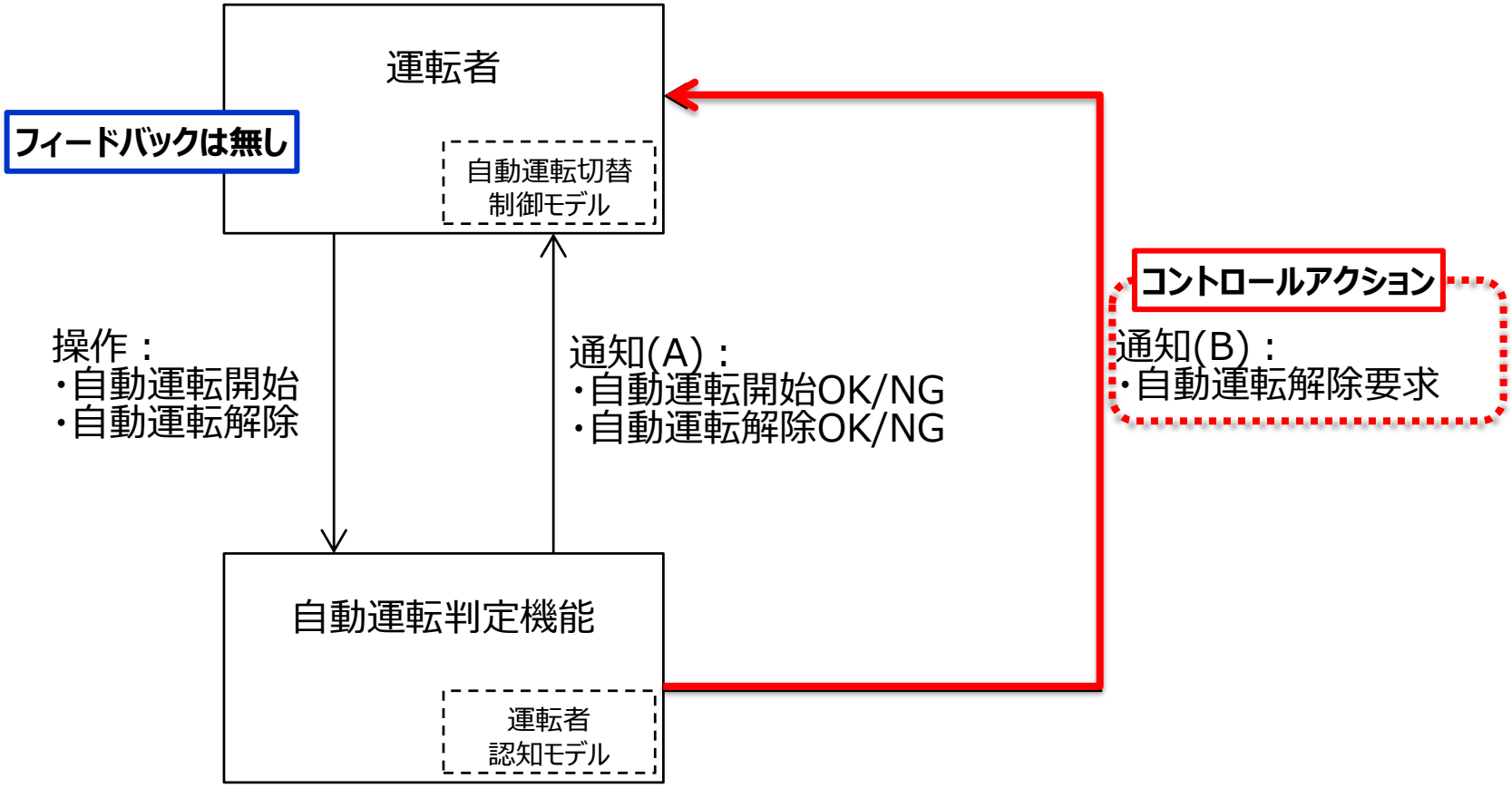
コントロールストラクチャの構築（STEP0-2）



※情報伝達手段は限定せず、視覚・聴覚・触覚による情報伝達全般を対象
※網羅的な検証とするため、詳細な仕様策定はしない

STAMP/STPAによる分析

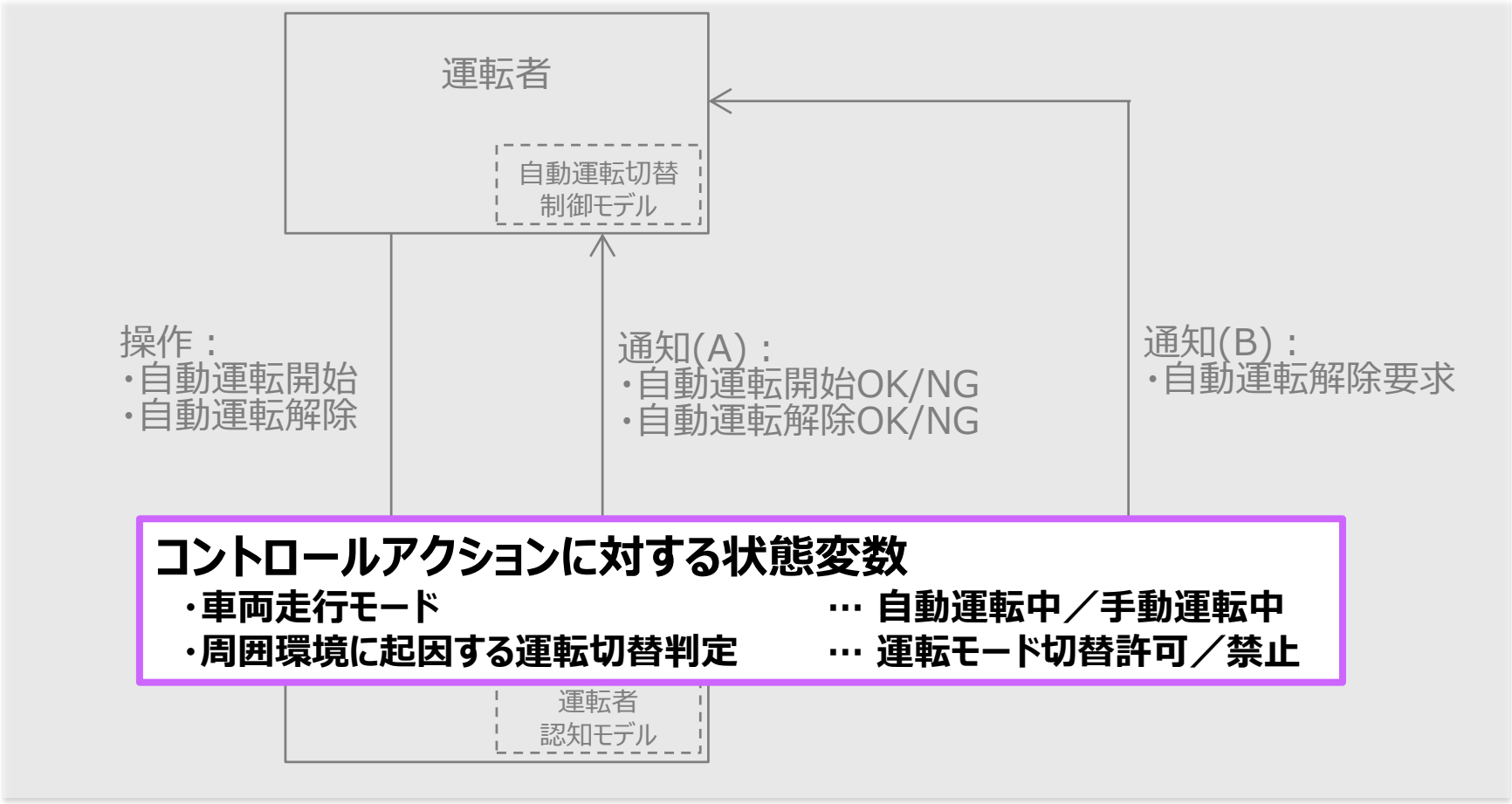
コントロールストラクチャの構築（STEP0-2）



※情報伝達手段は限定せず、視覚・聴覚・触覚による情報伝達全般を対象
※網羅的な検証とするため、詳細な仕様策定はしない

STAMP/STPAによる分析

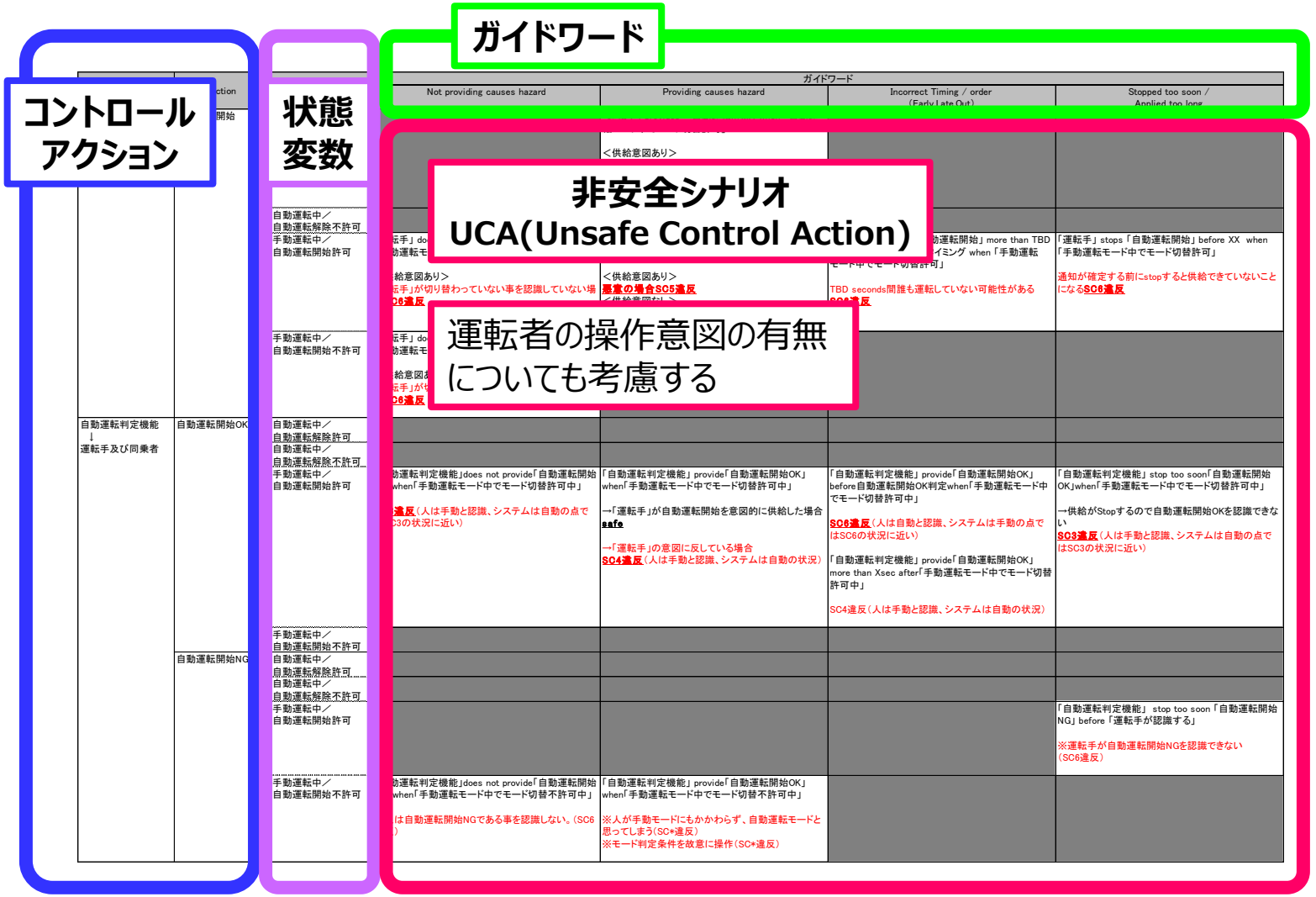
コントロールストラクチャの構築（STEP0-2）



※情報伝達手段は限定せず、視覚・聴覚・触覚による情報伝達全般を対象
※網羅的な検証とするため、詳細な仕様策定はしない

STAMP/STPAによる分析

ミスユースに関連する非安全シナリオの抽出（STEP1）



コントロールアクション		状態変数	ガイドワード: Not providing causes hazard	Providing causes hazard	Incorrect Timing / order (Early, Late, Out)	Stopped too soon / Applied too long
				＜供給意図あり＞		
		自動運転中／自動運転解除不許可 手動運転中／自動運転開始許可	転手」do 動運転モ ＜給意図あり＞ 転手」が切り替わっていない事を認識していない場 C6違反	＜供給意図あり＞ 悪意の場合SC5違反 ＜供給意図なし＞	動運転開始」more than TBD イミング when「手動運転 モード中でモード切替許可」 TBD seconds間誰も運転していない可能性がある SC4違反	「運転手」stops「自動運転開始」before XX when「手動運転モード中でモード切替許可」 通知が確定する前にstopすると供給できていないことになるSC6違反
		手動運転中／自動運転開始不許可	転手」do 動運転モ 給意図あ 転手」が C6違反			
自動運転判定機能 ↓ 運転手及び同乗者	自動運転開始OK	自動運転中／自動運転解除許可 自動運転中／自動運転解除不許可 手動運転中／自動運転開始許可	動運転判定機能」does not provide「自動運転開始 when「手動運転モード中でモード切替許可中」 違反（人は手動と認識、システムは自動の点で C3の状況に近い）	「自動運転判定機能」provide「自動運転開始OK」 when「手動運転モード中でモード切替許可中」 →「運転手」が自動運転開始を意図的に供給した場合 safe →「運転手」の意図に反している場合 SC4違反（人は手動と認識、システムは自動の状況）	「自動運転判定機能」provide「自動運転開始OK」 before自動運転開始OK判定when「手動運転モード中でモード切替許可中」 SC6違反（人は自動と認識、システムは手動の点ではSC6の状況に近い） 「自動運転判定機能」provide「自動運転開始OK」 more than Xsec after「手動運転モード中でモード切替許可中」 SC4違反（人は手動と認識、システムは自動の状況）	「自動運転判定機能」stop too soon「自動運転開始OK」when「手動運転モード中でモード切替許可中」 →供給がStopするので自動運転開始OKを認識できない SC3違反（人は手動と認識、システムは自動の点ではSC3の状況に近い）
		手動運転中／自動運転開始不許可				
	自動運転開始NG	自動運転中／自動運転解除許可 自動運転中／自動運転解除不許可 手動運転中／自動運転開始許可				「自動運転判定機能」 stop too soon「自動運転開始NG」before「運転手が認識する」 ※運転手が自動運転開始NGを認識できない（SC6違反）
		手動運転中／自動運転開始不許可	動運転判定機能」does not provide「自動運転開始 when「手動運転モード中でモード切替不許可中」 は自動運転開始NGである事を認識しない。（SC6 ）	「自動運転判定機能」provide「自動運転開始OK」 when「手動運転モード中でモード切替不許可中」 ※人が手動モードにもかかわらず、自動運転モードと思ってしまう（SC*違反） ※モード判定条件を故意に操作（SC*違反）		

STAMP/STPAによる分析

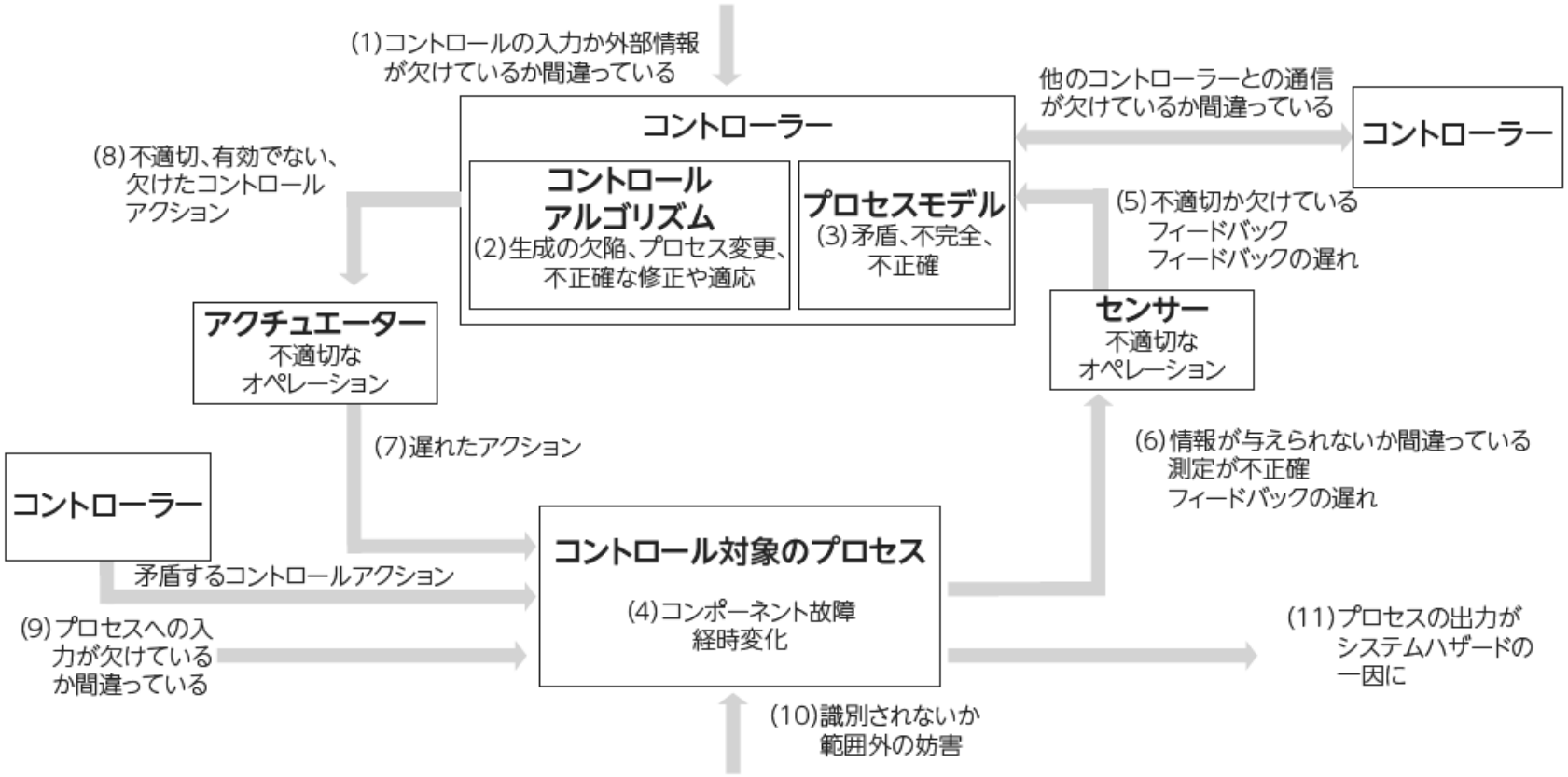
ミスユースに関連する非安全シナリオの抽出（STEP1）

コンポーネント間	Action	context	ガイドワード Not providing causes hazard	Providing causes hazard	Incorrect Timing / order (Early,Late,Out)	Stopped too soon / Applied too long
運転者 ↓ 自動運転判定機能	自動運転解除を通知 （＝手動運転開始を通知）	自動運転中 ／ 自動運転解除許可	「運転者が」 does not provide 「自動運転解除」 when 「自動運転モード中でモード切替許可」 Safe 運転者の意図が無い場合 **安全制約違反** 運転者が意図している場合 切り替わっていないことを認識していない	「運転者が」 provides 「自動運転解除通知を」 when 「自動運転モード中でモード切替許可」 **安全制約違反** 運転者の意図が無い場合 Safe 運転者が意図している場合	N/A 「運転者が」 provides 「自動運転解除通知を」 before 「自動運転切替」 Safe	N/A 「運転者が」 stopped too soon 「自動運転解除通知を」 before 「自動運転中で切替許可判定条件に入る」 Safe

安全制約
運転者が意図しない状況では自動運転モードを切り替えない
運転者が十分追従できるタイミングで意図する自動運転モードに切り替える、もしくは運転者の意図（操作）と車両状態の不一致がある場合は運転者に気付かせる

STAMP/STPAによる分析

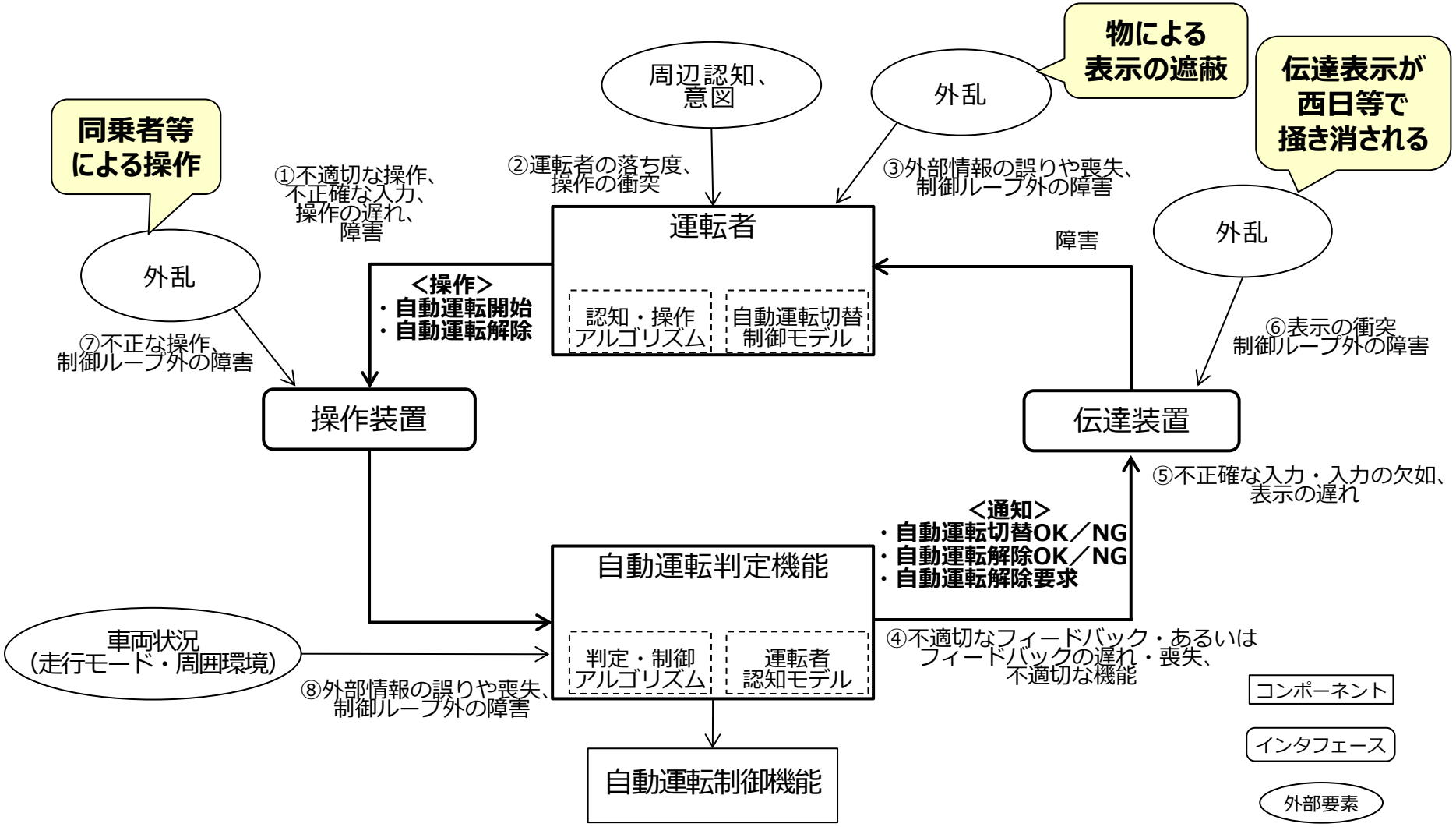
非安全シナリオに対するハザード要因の抽出（STEP2）



引用元：はじめてのSTAMP/STPA～システム思考に基づく新しい安全解析手法～

STAMP/STPAによる分析

非安全シナリオに対するハザード要因の抽出（STEP2）



STAMP/STPAによる分析

非安全シナリオに対するハザード要因の抽出（STEP2）

非安全シナリオ

ガイドワード

ハザード要因
HCF(Hazard Causal Factor)

非安全なコントロールアクション	適合、不完全、または不正確なプロセスモデル、不適切な操	コンポーネントの不具合、経年による変化	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	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	操作の遅れ	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の喪失	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	未確認、または範囲外の障害
「運転手」provides 「自動運転開始」when「手動運転モード中でモード切替許可」 ＜供給意図あり＞ **悪意の場合SC5違反**	N/A				N/A	N/A	N/A	・同乗者が悪意を持って不許可→許可にする(ex.センサ、カメラを操作) ・同乗者が悪意を持って操作端に触れる
〃 ＜供給意図なし＞ **SC4違反**	・動運転操作中、意図せず操作してしまう ・動運転操作中、意図せず操作端に触れてしまう ・サイバー攻撃	端に触れてしまう			N/A	N/A	N/A	・同乗者が意図せず操作端に触れる(ex.寝ている)
「自動運転判定機能」provide「自動運転開始OK」when「手動運転モード中でモード切替不可中」 ※人が手動モードにもかかわらず、自動運転モードと思ってしまう(SC*違反) ※モード判定条件を故意に操作(SC*違反)	N/A	・運転不切替許可の期間で、運転手が、別の伝達物(e.g.表示物)をOK判定と誤認識してしまう。	N/A	・自動運転判定機能(HMI表示側)が故障し、運転切替不許可の期間で、OK表示してしまう。	N/A	・運転不切替許可の期間で、自動運転判定機能の制御が不適切なため、OK指令を出してしまう。 ・運転不切替許可の期間で、自動運転判定機能が誤認識し、	N/A	・インバネなどの伝達経路に意図的に細工を施す →論理反転改造など
「自動運転判定機能」 stop too soon「自動運転開始NG」before「運転手が認識する」 ※運転手が自動運転開始NGを認識できない (SC6違反)	N/A	・運転切替不許可の期間で、NG表示後すぐに運転手が非覚醒状態になり、NG表示に気づかない(供給されない) ・	N/A	・自動運転判定機能(HMI表示側)が故障しNG判定後、既定の時間より早くNG表示をOFFしてしまう。	N/A	・自動運転判定機能の制御が不適切なため、NG判定後、既定の時間より早くNG指令をOFFしてしまう。	N/A	・NG表示後すぐに障害物などにより、目視確認できなくなる(悪意アリ/ナシ) ・インバネなどの伝達経路に意図的に細工を施す

ハザード要因：合計63個抽出

63個を整理して、グループ分けを実施

STAMP/STPAによる分析

非安全シナリオに対するハザード要因の抽出（STEP2）

非安全シナリオ	①不適切な操作、不正確な入力、操作の遅れ、障害	②運転者の落ち度、操作の衝突	③外部情報の誤りや喪失、制御ループ外の障害	④不適切なフィードバック・あるいはフィードバックの遅れ・喪失、不適切な機能	⑤不正確な入力・入力の欠如、表示の遅れ	⑥表示の衝突、制御ループ外の障害	⑦不正な操作、制御ループ外の障害	⑧外部情報の誤りや喪失、制御ループ外の障害
「運転者が」 provides 「自動運転解除通知を」 when 「自動運転モード中でモード切替許可」 **安全制約違反** 運転者の意図が無い場合	・他の操作をしようとして、誤って自動運転解除通知操作をする ・その操作が自動運転解除操作と知らずに操作する	・突然の病気等で倒れた拍子に自動運転解除通知操作をしてしまう					・同乗者等により、運転者が知らないうちに自動運転解除通知が操作される	

STAMP/STPAによる分析

ハザード要因と安全要件の抽出

	ハザード要因
1	運転者に意図が無くモード切替操作が実施され、モードが切替ったことを運転者が認識していない
2	運転者が自動運転車の知識が無く、モード切替操作と知らずにモード切替操作が実施されてしまう
3	運転者が意図を持ってモード切替操作を実施したが、モードが切り替わらないことを運転者が認識していない
4	運転者に表示の内容が伝わらない
5	運転者に伝達音の内容が伝わらない
6	運転者が表示の内容を誤認識してしまう
7	不適切な表示により、運転者が運転の誤操作をしてしまう（手動運転中）
8	自動運転切替動作に対する運転者の対応遅れ
9	環境認識機能（外部センサ、ドライバモニタ等）の誤認識により、実際の環境状況と判定結果が不一致

運転者が運転モードを認識していない

運転者が運転モードを認識している

※機器の故障も抽出したが、スコープ外として除外した

STAMP/STPAによる分析

ハザード要因と安全要件の抽出

	ハザード要因	安全要件
1	運転者に意図が無くモード切替操作が実施され、モードが切替ったことを運転者が認識していない	・運転者が認識していない状態ではモード切替操作が行われても、モード切替をしない
2	運転者が自動運転車の知識が無く、モード切替操作と知らずにモード切替操作が実施されてしまう	・運転者は自動運転車の機能について熟知していること
3	運転者が意図を持ってモード切替操作を実施したが、モードが切り替わらないことを運転者が認識していない	・運転者の意図に対し適切な操作を促す操作端であること
4	運転者に表示の内容が伝わらない	・システム意図を確実に運転者に伝えること
5	運転者に伝達音の内容が伝わらない	・システム意図を確実に運転者に伝えること
6	運転者が表示の内容を誤認識してしまう	・運転者に誤認識させない表示であること
7	不適切な表示により、運転者が運転の誤操作をしてしまう（手動運転中）	・運転者を驚かせない表示を供給すること
8	自動運転切替動作に対する運転者の対応遅れ	・運転者へ運転権限を委譲するまでの時間と切替制御が適切であること
9	環境認識機能（外部センサ、ドライバモニタ等）の誤認識により、実際の環境状況と判定結果が不一致	・実際の環境状況と判定結果に不一致無いこと

※ハザード要因を制御・除去し安全となるために必要な条件

STAMP/STPAによる分析

ハザード要因と安全要件の抽出

	ハザード要因	安全要件
1	運転者に意図が無くモード切替操作が実施され、モードが切替ったことを運転者が認識していない	・運転者が認識していない状態ではモード切替操作が行われても、モード切替をしない

安全要件を実現するための
具体的な課題を抽出

課題
①不意な操作では作動しないHMIの配置
②不意な操作で作動しない手法確立
③認識してない状態をどう認識するか
④セキュリティ（ハッキング対策）
⑤耐環境性の保証
⑥同乗者による操作をどう認識するか
⑦意図しないモード切り替えの禁止 （オーバーライド仕様）

※ハザード要因を制御・除去し安全となるために必要な条件

STAMP/STPAによる分析

課題の抽出と整理

	ハザード要因	安全要件	課題
1	運転者に意図が無くモード切替操作が実施され、モードが切替ったことを運転者が認識していない ・無意識（非覚醒、睡眠、他事中、余所見、意図しないオーバーライド） ・病気等で倒れた時に誤って操作 ・同乗者による操作（モード切替操作を知っている、知っていないに関わらない、悪意による操作） ・同乗者がモード切替と知っていて、運転者が見てないときに操作実施 ・外部の音、衝撃に注意が向いたときに、誤って操作 ・車室内の物が飛来してきて、操作実施 ・外部からのハッキングにより、操作実施 ・落雷などのノイズにより、操作実施	・運転者が認識していない状態ではモード切替操作が行われても、モード切替をしない	①不意な操作では作動しないHMIの配置 ②不意な操作で作動しない手法確立 ③認識してない状態をどう認識するか ④セキュリティ（ハッキング対策） ⑤耐環境性の保証 ⑥同乗者による操作をどう認識するか ⑦意図しないモード切り替えの禁止 （オーバーライド仕様）
2	運転者が自動運転車の知識が無く、モード切替操作と知らずにモード切替操作が実施されてしまう ・モード切替操作であると知らなかった（モード切替操作をそもそも知らない） ・モード切替操作だと気づかなかった（モード切替操作があることは知っている）	・運転者は自動運転車の機能について熟知していること	①操作端の統一の要否 ②運転者への教育の要否
3	運転者が意図を持ってモード切替操作を実施したが、モードが切り替わらないことを運転者が認識していない ・運転者の操作間違いにより、モード切替が伝達されない（例：ボタン押しきれてない、レバーが逆） ・運転者が操作方法[illegible] ・運転[illegible]	・運転者の意図に対し適切な操作を促す操作端であること	①操作のし易さ　（配置、確実性） ②ソフトウェア要件への適合性確認 ③運転者への教育の要否 ④障害物の検知の要否 [illegible]端の故障検知 [illegible]者のシステム依存度の把握

ハザード要因　：大分類9種類
　　小分類63個
課題総数　　：39個

STAMP/STPAによる分析

操舵系に関するミスユース課題の選別

本事業

自動走行ビジネス検討会

経産省、国交省が設置している、自動走行において競争力を確保し世界の交通事故の削減等に貢献するために必要な取組みを、産官学で検討を行う検討会。

戦略的イノベーション創造プログラム（SIP）

科学技術イノベーションを実現するために創設され、府省・分野を超えた横断型のプログラム。

※SIP：Cross-ministerial Strategic Innovation Promotion Program

SIPの自動運転関係ヒューマンファクター事業でも
同様の研究を行っているため、課題の棲み分けを実施

STAMP/STPAによる分析

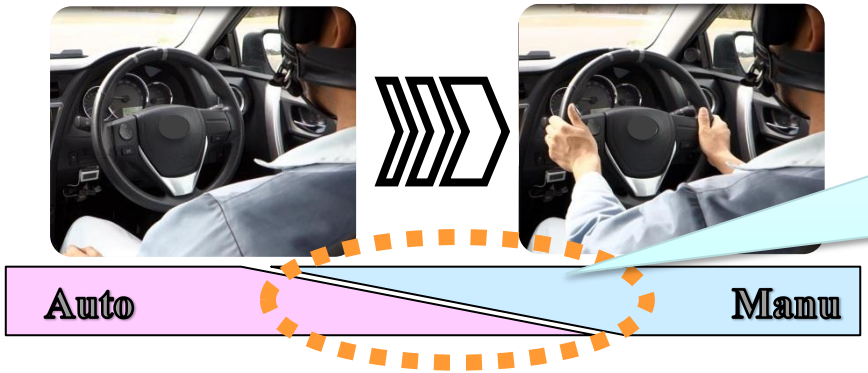
操舵系に関するミスユース課題の抽出

課題A　運転者が意図しない自動運転モード解除の回避
（オーバーライドにおける課題）

オーバーライド：機械の動作を人間が意思を持って打ち消すこと

意思を持たなくてもオーバーライドと**誤判定され、**
自動運転が勝手に解除され、アクシデントへ至ることを懸念

課題B　システムが運転者へ運転権限を委譲する際の適切な操舵トルク切替制御
（自動から手動への切替え時の課題）



権限委譲時の操舵トルク制御の
不適切な遷移仕様により、運転者の
不安定な操舵を招き、**アクシデントに**
至ることを懸念

発表内容

1．背景および目的

2．ミスユース安全設計

3．STAMP/STPAによる分析

4．課題に対する取組み

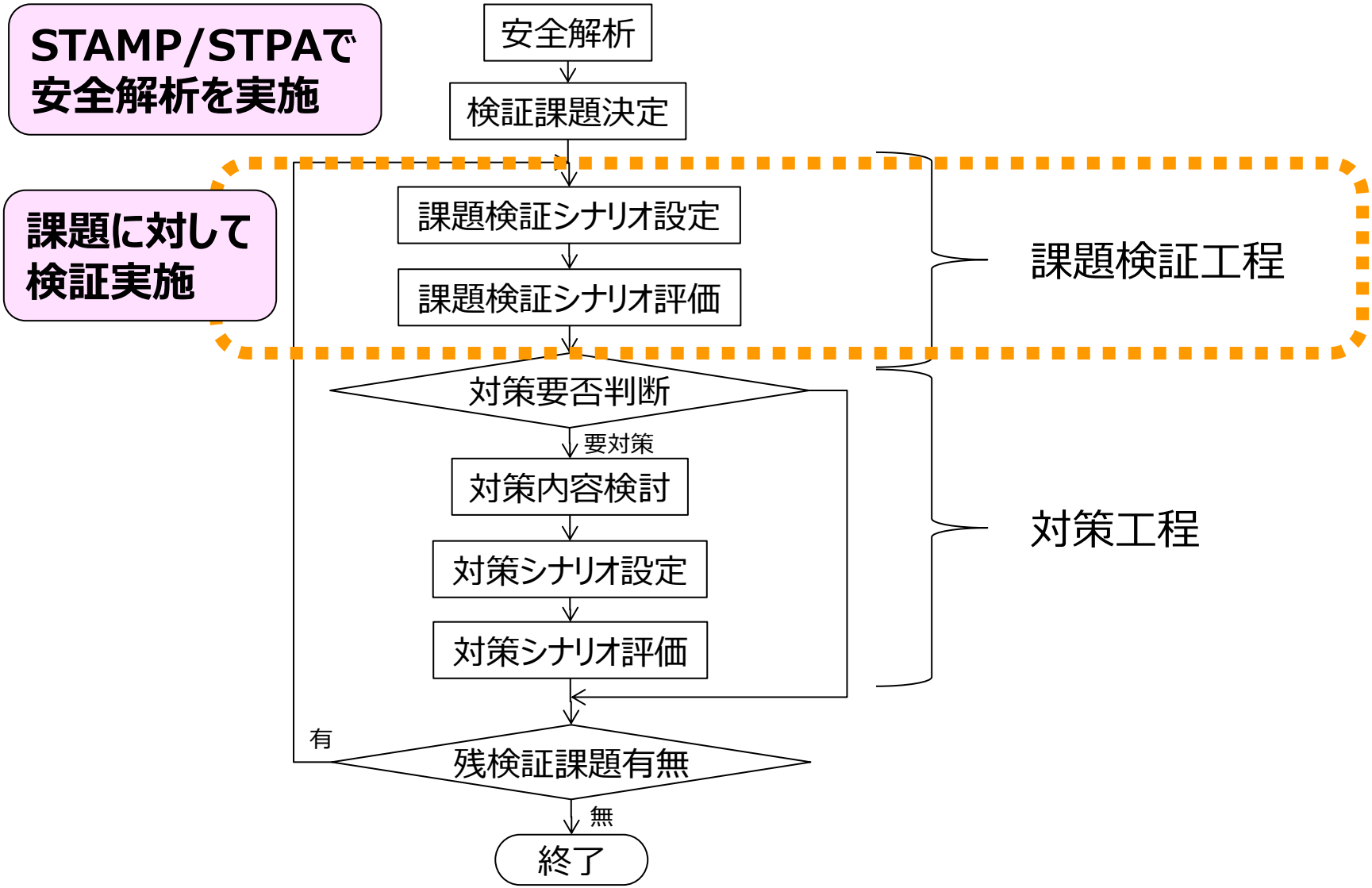
5．まとめ

課題に対する取組み

提案するミスユース安全設計検討プロセス

STAMP/STPAで安全解析を実施

課題に対して検証実施



課題に対する取組み

抽出した操舵系に関するミスユース課題

課題A　運転者が意図しない自動運転モード解除の回避
（オーバーライドにおける課題）

オーバーライド：機械の動作を人間が意思を持って打ち消すこと

意思を持たなくてもオーバーライドと**誤判定され、**
自動運転が勝手に解除され、アクシデントへ至ることを懸念

オーバーライドで自動運転解除する機能あり

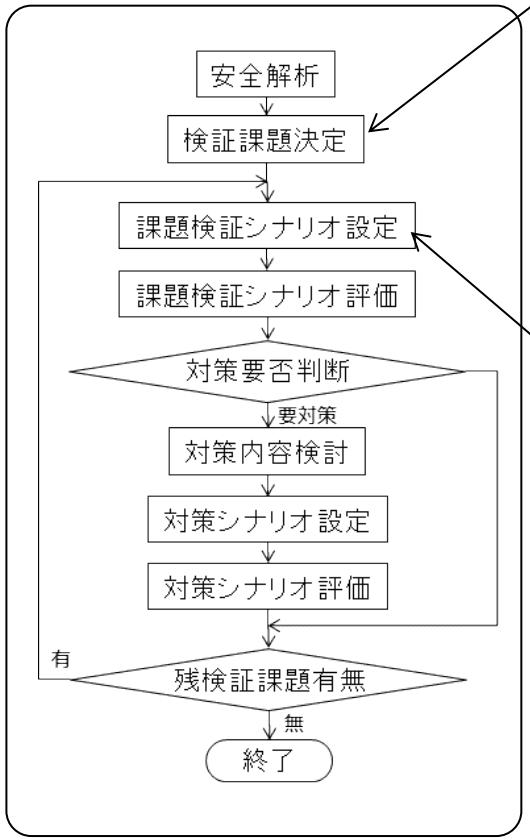
課題B　システムが運転者へ運転権限を委譲する際の適切な操舵トルク切替制御
（自動から手動への切替え時の課題）

権限委譲時の操舵トルク制御の
不適切な遷移仕様により、運転者の
不安定な操舵を招き、**アクシデントに**
至ることを懸念

課題に対する取組み

抽出した操舵系に関するミスユース課題

＜提案する検証プロセス＞



＜抽出した検証課題＞

★**運転者が意図しない自動運転モード解除の回避（課題A）**

★システムが運転者へ運転権限を委譲する際の適切な操舵トルク切替制御（課題B）
- ・運転モード切替を誤操作しないHMIシステムのデザイン
- ・運転モード切替時の運転者の状態認識方法
- ・周辺環境により誤動作しない運転モード切替システム構築
- ・運転者の無知による運転モード状態の誤解の回避
- ・etc

＜課題検証の設定項目＞

〔課題A〕
- ・意図しない自動運転モード解除要因

★**音、衝撃に驚き操舵入力**
- ・後部座席の物を取ろうとして操舵入力
- ・急病で倒れてハンドルを保舵
- ・etc

操舵入力方法

★**ハンドルの下端から上方向に手で操舵**
- ・ハンドルの上端から下方向に手で操舵
- ・ハンドル下端に膝が当たって操舵
- ・etc

走行シチュエーション

★**高速R380@100km/hで走行中**
- ・一般道低速で交差点右折（or左折）
- ・急カーブ直前の直線走行中
- ・etc

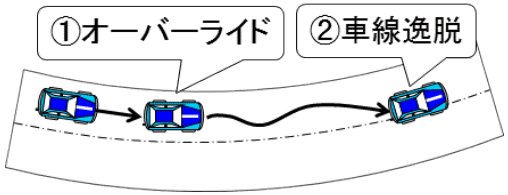
具体例(★印)を用いてプロセスの手順を説明

課題に対する取組み

課題A：実験条件

具体例として「音や衝撃に驚いて、操舵する」という意図しないオーバーライドを抽出

良否判定条件



○ 逸脱しない：安全
× 逸脱する：非安全

操舵系においては車両の横移動に着目し、
車線逸脱するかどうかを判定基準とした

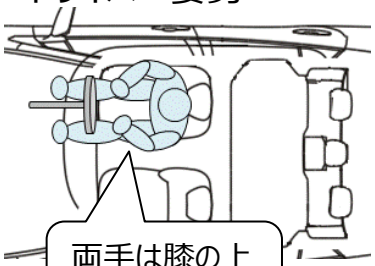
走行状態

・定常円旋回R380m
・100km/h

ワーストケースとして、高速走行中に
意図しないオーバーライドが発生する
ことを想定した

ドライバー状態

・ドライバー姿勢



・操舵方法

ハンドルに下から手を当てて
瞬間的な操舵トルクを掛ける
その後ハンドルに触れない

網羅的または最悪条件を検討すべきだが
複数の候補から具体例一つ抽出し、
プロセスの手順を説明した。

課題に対する取組み

課題A：実験結果

オーバーライド判定条件

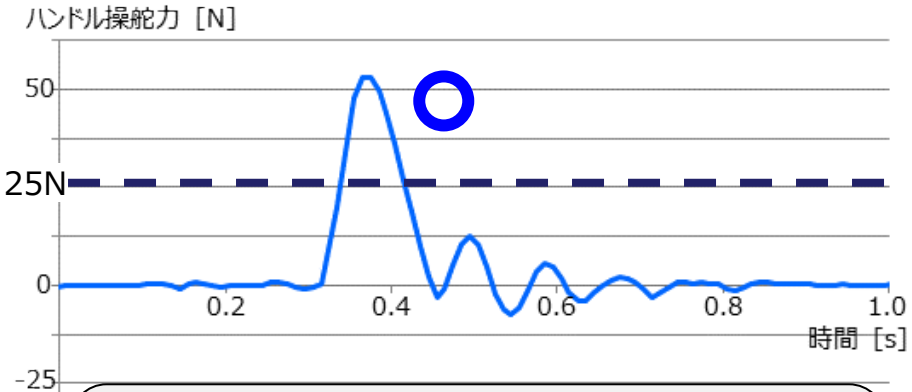
・ハンドル操舵力25N以上
・継続時間0.1s

ACSFのオーバーライド判定条件(50N以下)から判定条件を検討

ACSF：Automatically commanded Steering Function

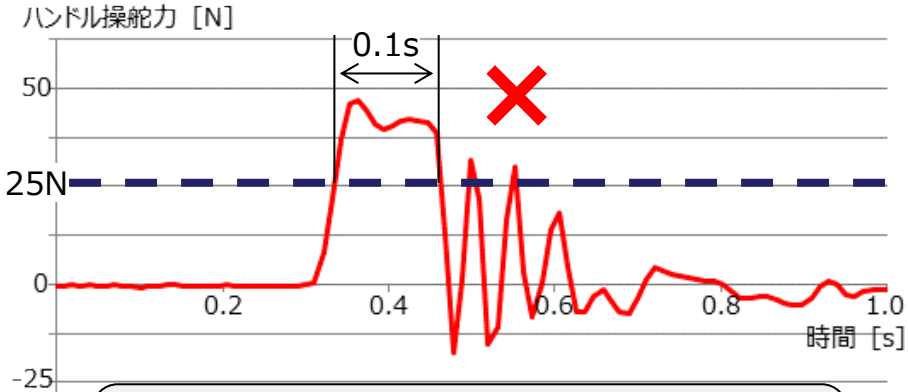
実験結果（逸脱しない：安全）

○ 逸脱しない：安全
× 逸脱する：非安全



25Nを超えるが、継続時間が0.1s未満であるので、オーバーライド判定せずに車線逸脱しなかった

実験結果（逸脱する：非安全）



25N以上が0.1s継続したため、オーバーライド判定され車線逸脱した

発表内容

1．背景および目的

2．操舵系に関するミスユース安全設計

3．STAMP/STPAによる分析

4．課題に対する取組み

5．まとめ

まとめ

STAMP/STPAによる分析作業

・ガイドワードを参考とし、網羅的に抽出可能な手法であるが、
各ステップでの抽出項目には個人の技量の差が包含される
⇒ 検討を進める途中で、新しい検討項目が抽出された

【新しい検討項目の一例】

	ハザード要因	安全要件	課題
8	自動運転切替動作に対する運転者の対応遅れ ・同乗者による切替操作が不意であり、運転者がその切り替わりに対応できない ・意図しない切替操作に対し、運転者がその切り替わりに対応できない	・運転者へ運転権限を委譲するまでの時間と切替制御が適切であること	①運転権限委譲までの時間仕様 ②運転切り替え開始から完了までの制御仕様

・対象を限定しない状態でのミスユース課題抽出には有効な手段であると考える
・抜け漏れなく実施するには、繰返し検討を実施し技量を高める必要がある
・新たな気付きを抽出するには、高い技量が必要となる

ご清聴ありがとうございました