研究コース６

システム思考とレジリエンスエンジニアリングを用いた安全性分析の試行

リーダー：吉田　篤（東芝）　　藤原　真哉(NTT コミュニケーションズ)
里富　豊（ﾘｺｰ IT ｿﾘｭｰｼｮﾝｽﾞ）
研 究 員：鎌田　桂太郎(アイホン)　　黒田　知佳(ﾃｯｸｴﾝｼﾞﾝｿﾘｭｰｼｮﾝｽﾞ)
松崎　美保(TIS)　　西　啓行(富士通)
大森　裕介(ｴﾌﾟｿﾝｱｳﾞｧｼｽ)
主　査　：金子　朋子（国立情報学研究所）
副 主 査：髙橋　雄志（日本 AI システムサービス）
アドバイザー：佐々木　良一（東京電機大学）

研究概要

経時的な問題の抽出や要素間の関係性の図示，成功要因からの安全性分析技術で想定外を想定できるということを仮定し，AI を含んだシステムの安全性の検証を行った．実際に起きた自動運転レベル 3 の事故を事例にシステム理論の事故モデル STAMP に基づく事故分析手法 CAST とリスク分析手法 STPA，並びにレジリエンスエンジニアリングに基づくリスク分析手法 FRAM の 3 つの分析手法を効率的に運用することで想定外を想定した安全性向上を目指した．これらはそれぞれ異なる特徴をもち，1 つの事例に適用し比較した事例はない．さらに CAST 分析に，新たに 5 階層モデルの考え方を適応することを試みた．その結果，これらの分析手法により事故報告書にない改善勧告を導出することができた．

1. はじめに

AI・IoT を始めとした技術の革新により，多様性があり複雑な構成のシステムが登場してきている．我が国でも政府主体で自動走行ビジネス検討会を立ち上げ，自動走行の実現に向けた取組報告と方針を発表している[1]．

自動運転は，自動車に先駆けて航空宇宙分野や鉄道などで運用されているが，いくつもの事故事例が報告されている．その中で我々が着目したのは，想定外の事象によって引き起こされる事故である．AI は囲碁などのテーブルゲームで人間の想像を超えた勝利をし[2]ソフトウェアとしては進歩したものの，人や外部環境，物理システムを含む AI システムを安全に構築する際には，AI システムを構築する際には，システム思考やレジリエンスエンジニアリングの考えを適用し，刻一刻と前提となる環境や技術の変化に対応する分析や複雑なシステム要素間の関係性に基づく分析，失敗要因以外に着目した分析が必要になると考えた．

我々は，STAMP（Systems Theoretic Accident Model and Processes）/CAST（Causal Analysis based on System Theory），STPA（STAMP based Process Analysis），FRAM（Functional Resonance Analysis Method）といった手法で経時的な問題の抽出や要素間の関係性の図示，成功要因からの安全性分析といった課題解決ができると考えた．本稿では，事故事例として 2018 年 3 月にアリゾナ州で発生した Uber の自動運転システムの事故報告書[3]の内容（以下，事故報告書）を 3 つの分析手法を用いて改めて分析した．なお，本稿では実験において，事故報告書に記載されていない内容を想定外と位置付けている．

2. 関連技術

2.1. STAMP

Leveson が提唱した STAMP モデルでは，システムの様々な階層でコントローラーと被コントロールプロセスに該当する要素が存在しており，それらの相互作用が適切に働くことによりシステムの安全が実現されるとする．STAMP モデルでは，アクシデントは相互作用が適切に働かないことによって起こり，具体的にはコントローラーから被コントロールプロセスへの必要な制御指示（以下，CA: Control Action）が適切に与えられないために起こるとしている．そして，不適切な CA が与えられる要因として，コントローラー自身が想定する被コントロールプロセスの状態が，実際の被コントロー ルプロセスの状態を正しく反映できていないことが主要な要因であるとしている．たとえコントローラーも被コントロールプロセスも故障せずに，仕様通りに正しく動作していても，このような認識の不整合により不適切な CA が与えられ，最終的にアクシデントにつながるというアクシデントモデルなのである[4]．また，コンポーネント間の CA，フィードバックデータといった相互作用を分析するために，制御構造図（以下，CS：Control Structure）を構築し使用する．

2.1.1. STPA

Leveson 等が提唱した STPA は STAMP アクシデントモデルを前提として，システムのアクシデントの可能性が潜在している状態（ハザード）とその要因を事前に分析するための新しい安全分析手法である[4]．従来は，FTA（Fault Tree Analysis）や FMEA（Failure Mode and Effect Analysis）の手法が用いられてきたが，これらは，単一コンポーネントの分析には有用であるが,現代の相互作用が複雑なシステムの安全分析においては十分ではないため，新しいアクシデントモデルによる分析手法が必要とされた．

STPA の手法により早すぎる遅すぎるというチェック観点からの経時的なハザード要因洗い出したり，また登場人物とハザードを照らし合わせ分析に不足がないかを繰り返し確認したりすることによって「想定外」を改善勧告することが出来るのではないかと考えた．

2.1.2. CAST

Leveson が提唱した CAST は，事故全体の理解のためのフレームワークとプロセスを提供し，事故の原因分析をシステムの構成要素と関連する CA の弱点にフォーカスして行う．CAST を用いることで，人を含むシステムを構成する要素間の関係性や，システムが置かれた状況(コンテキスト)を考慮したシステム全体への事故分析ができるのではないかと期待されている[5]．

上記の特徴から我々はこの手法が，複雑な構成要素を持つ自動運転システムの事故の分析に適用できると考えた．

2.1.3. STAMP/S&S

STAMP S&S における STAMP とは，System Theoretic Architecture Model and Process となり従来の STAMP を拡張した金子の提案である.S&S は,Safety ,Security の他,Society, Stakeholder, Service, System, Software の 5 階層のアーキテクチャと，Specification, Standard, Scenario の略称を指す[6]．その方法はシステムを 5 層に対象をモデル化し，自然環境や社会規範などの社会自体や AI システムを含めた世界をシステム思考でとらえることができるリスクと事故等の分析方法である．

従来の STAMP 事例ではシステムレベルが中心であり，自然や社会環境,ソフトウェアの対象の特徴にあわせた詳細な相互分析までは触れられていない．我々は，この手法の 5 階層モデルという特徴に着目し，適用することで，Society から Software に至るまでの階層において法制度や AI システムを含む複雑な構成要素間の関係を考慮した分析が可能になると考えた．

2.1.4. FRAM

Hollnagel が提唱したレジリエンスエンジニアリングにおいて，システムのレジリエンス向上のためには，Monitor，Respond，Learn，Anticipate の 4 つの能力(以下，4 つの機

能)の向上が有効であることを主張した[7]．FRAM とは，レジリエンスエンジニアリングにおける分析手法であり，動的システムにおけるリスクの特定などに用いられる．FRAM では，複数の機能とそれらの関係によって分析対象のモデルを記述し，各機能が互いにどのように影響しているか（機能共鳴）を分析する．

FRAM を安全分析に適用する上での従来の手法と異なる特徴は，分析対象における失敗事象を予め定義しない点である．レジリエンスエンジニアリングの考え方において，安全は意図しない入力に対する柔軟性によって実現され，失敗はその柔軟性と他の要因との予期せぬ相互作用によって生じる．FRAM ではこの考え方に基づき，予め失敗事象を定義せず，各機能の関係性及び相互の入出力の変動に着目した分析を行う．我々は，成功要因から分析を行うことで，従来とは別の観点の結果が得られると考えた．

3. 安全性分析方法の検証実験

本実験では，AI を含むシステムの安全性分析を行ことで，想定外を想定する分析方法を検証する．そのために，実際の事故事例に対して複数の安全性解析手法を用いて多角的な観点で分析を行う．具体的には，事故報告書を用い，安全解析手法として STAMP/CAST，STPA，FRAM の 3 つの手法を用いて分析を行い，改善勧告を導出した．各分析手法をどのように用いて分析を行ったかは 3.1 節にて解説する．

なお，自動運転のレベルは参考文献[8]の内容に準じ，事故報告書はレベル 3 に該当する．

3.1. 本実験における分析手法

3.1.1. STAMP/CAST を用いた分析

事故理由及び事故発生を許した安全制御構造の弱点を，経時的な変遷を含めて明らかにすることを目的に，CAST を用いて自動運転レベル 3 の事後分析を行った．俯瞰的に問題点を抽出するため，STAMP S&S における 5 階層モデルのアーキテクチャに基づき事故に関わる全ての構成要素に対して分析を行った．この CAST への 5 階層モデルの適用及び AI システムを含めた分析は，システム理論に基づく事故分析手法として過去事例にない新規性のある試みである．本分析における手順を以下に示す．

(1) 図 1 で示す CAST HANDBOOK[9]に書かれた手順を参考に事故分析を行う．本分析では分析の観点として，STEP 2 から 4 の手順に S&S の 5 階層モデルの考え方を加えた．

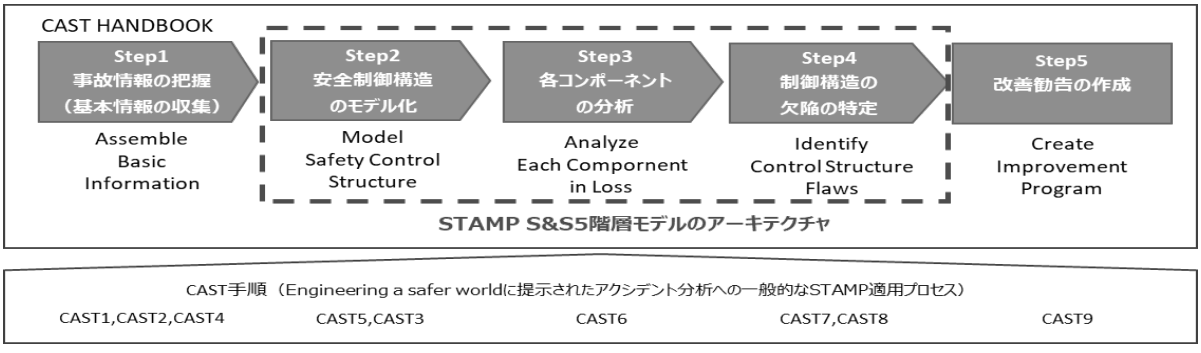


図 1： CAST 分析のステップ

(2) 抽出した改善勧告が想定外のものであるかの検証を行う．

3.1.2. STAMP/STPA を用いた分析

事故報告書のシステム構成をもとに想定した自動運転レベル 5 のシステムに対して STAMP/STPA を用いてリスク分析を行う．その結果として，リスクを回避できる改善勧告ができるのか，事故報告書では考慮していないリスクを抽出しかつ改善勧告につなげることができるのかを検証した．本実験における分析手順を以下に示す．

手順 1：自動運転レベル 5 の機能として，人間の機能（自動運転レベル 0）をベースとし機能をピックアップ

手順 2：STEP0 は，前提条件として Uber の事故情報を設定.
それ以外の STEP0 から STEP1 は通常の STAMP/STPA 手順に同じ.
手順 3：STEP2 の HFC は Uber の事故情報とする.
手順 4：対策検討から「想定外の改善勧告」を提案.

3.1.3. FRAM を用いた分析

人間が運転する場合の成功要因を自動運転に反映させる事で，安全性が高められる視点を検討する．以下の手順で分析を行う.

① 人間が自動車を運転する場合の中心となる機能を決定する
② 中心機能の 6 要素（「Input」「Precondition」「Resource」「Time」「Time」「Output」）に関連する機能へ広げモデル化する
③ 人間が運転する部分を自動運転（AI）に置き換える
④ 4 つの機能の追加を検討する

本分析のポイントは，機能と機能がどのように影響しあい，依存しあい，強めあい，弱めあっているのか（機能共鳴）を分析することであり，個別のコンポーネントやデータではなく，統合的な視点でネットワークトポロジーに着目し，システムの失敗要因を定義せず，成功要因に着目することにある.

3.2. 実験結果

3.2.1. CAST を用いた分析

【Step1】事故情報の把握（基本情報の収集）

CAST1，2：アクシデントを「歩行者との衝突が発生した」と定義し，アクシデントとなりうるハザードとハザードの裏返しとなる安全制約を導出した.

CAST4：What-Why 分析により What（何が起きたのか）と Why（原因究明のため明らかにしたいこと）の観点で，各イベントの発生理由に対する質問を生成した．その結果を表 1 に示す（詳細は参考文献[10]を参照）.

表 1：アクシデント／ハザード／安全制約／イベントチェーンと質問生成結果

アクシデント	ハザード	安全制約	What?:何が起きたのか	Why?:原因究明の為明らかにしたいこと
歩行者との衝突が発生した	緊急時に衝突を回避しない	緊急時には衝突を回避をする	移動履歴を考慮していない	なぜ、考慮しなかったのか

【Step2】安全制御構造のモデル化

CAST5：各コンポーネントを事実に基づき 5 階層に分類し欠陥分析した．その結果を表 2 に示す（詳細は参考文献[10]を参照）.

表 2：具体的コンポーネントレベルでの分析結果–

カテゴリ	事故発生対象	CAST5-1	CAST5-2	CAST5-3	CAST5-4
		安全上の責務(責任)	非安全なCA	プロセス/メンタルモデルの欠陥	意思決定された状況・背景
Software	知覚プロセス パーセプション	歩行者を正しく歩行者として分類する	歩行者を正しく歩行者として分類されなかった	システムの設計には信号無視の歩行者への配慮がない。	歩行者は車道を渡ってはならない（アリゾナ州）

CAST3：対象システムの安全性を保つために存在すると考えられる安全制御構造を，5 階層のアーキテクチャを用いた安全 CS として作成した．その結果を図 2 に示す（詳細は参考文献[10]を参照）.

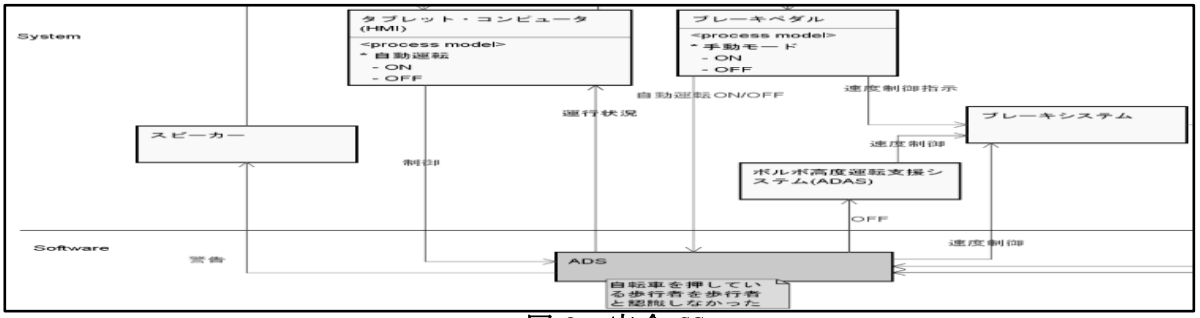


図 2：安全 CS

【Step3】抽象的事例（論理モデルの分析）の分析

CAST6：コンポーネントを論理モデルに概念化，5 階層に分類し，安全上の責務と非安全なコントロールアクション，及びプロセス・メンタルモデルの欠陥と背景を抽出した．その結果を表 3 に示す（詳細は参考文献[10]を参照）．

表 3：抽象的コンポーネントレベルでの分析結果

カテゴリ	高位レベルの事象（抽象的事象）	CAST6-1 安全上の責務（責任）	CAST6-2 非安全なCA	CAST6-3 プロセス/メンタルモデルの欠陥	CAST6-4 意思決定された状況・背景
Software	認識技術	対象物を正しく分類する	対象（歩行者）を正しく判断できない条件があった	信号無視の歩行者を歩行者として認識する設計になっていない	法律では、歩行者は車道を渡ってはならないとなっている

【Step4】制御構造の欠陥の特定

CAST7:各コンポーネントの特定した欠陥と特徴を，5 階層及び要因の観点で分類した．

CAST8:安全 CS の時間経過による動的な特性や変化，及び長期間での弱化を識別した．その結果を表 4 に示す（詳細は参考文献[10]を参照）．

表 4：システムの俯瞰分析結果

欠陥	コンポーネント	Society	Stakeholder	Service	System	Software	CAST7 安全リスク評価・冗長性	CAST7 設計不備・考慮漏れ	CAST7 安全なマネジメントシステムの設計	CAST8 経時的な変化とダイナミクス
対象の移動方向を正しく認識しなかった	予測機能	－	◎ 設計不備	－	－	● 設計不備	◎ 設計不備	● 設計不備	－	－

【Step5】改善勧告の抽出

CAST9：Step4 で抽出した欠陥に対して改善勧告を 32 件抽出した．その結果を表 5 に示す（詳細は参考文献[10]を参照）．

表 5：事例の特徴と分析から見える弱点とその改善案

特徴	分析から見える弱点	改善勧告案
設計に関するもの	車両と運転手とのIFについて緊急時には運転手の判断に基づく（依存した）設計であり「運転手は不安全な運転を行う」等の配慮が全体的に不足。	緊急時には、とっさの行動が運転手にはできないことを前提とし、「緊急時の自動運転が行う安全確保の行動」を定義する。

ここまでの分析で導出された改善勧告のうち，想定外のものがないかを確認したところ 18 件の想定外の改善勧告が導出できていることがわかった．その一部を以下に記す（詳細は参考文献[10]を参照）．①「人がルールを守る」「人が自発的行動を起こす」前提の対策になっているため，事故の抑制かゼロにするのか目的・目標の明確化が必要，②安全性およびリスクに対する評価･冗長性に対してより積極的な対応が必要,③自動運転(レベル 5 等)レベルに応じた免許制度（ドライバー，搭乗者の役割・責任等）や道路環境の実現等の運用面や法整備への対応が必要．以上のことから，CAST への 5 階層モデルの適用及び AI システム（自動運転レベル 5 等）を含めた分析は新規性のある試みであり，想定外を想定することができたと結論付けた．

3.2.2. STPA を用いた分析

CS（図 2）を見ると ADAS の機能が停止されていることがわかり，事故報告書からこの停止する CA は UCA（Unsafe CA）であることがわかる．また，ADAS の追加情報として機能が通行であったとしても時間的制約があることも判明しており,ガイドワードの「遅すぎる」により同様の改善勧告が導出できることがわかった．

手順 1 から表 6（詳細は参考文献[10]を参照）が示すような改善勧告を新規機能①から③に基づき導出することができた．

表 6：コンポーネント抽出表

レベル0	レベル5
運転者（目視）	センサー・カメラ・ライダー
運転者（聴覚）	新規機能①（聴覚）
運転者（嗅覚）	新規機能②（嗅覚）
運転者（体感）	新規機能③（体感）
運転者（思考）	AI

また，手順 2 の STEP0 から「ディープラーニング，ネットワーク，サイバーセキュリティ，交通ルール，インフラ整備」等が抽出され，手順 4 から表 7（詳細は参考文献[10]を参照）で示すように改善勧告を洗い出した．

表 7：対策表

現状（想定外）	改善勧告	ハザード
自動運転レベル 3 報告書では学習の記載なし	今後レベル5に向けて学習を繰り返し,外界情報のよる判別の精度・予測の制度をあげることに運転機能の向上となる	学習不足による判断ミス・予測不備よる事故・違反が起きる
	今後レベル5に向けて学習を繰り返し,誤情報を取り込む可能性があるがその場合,誤情報だという認識を与える必要がある	間違った学習による判断ミスよる事故・違反が起きる
自動運転レベル 3 報告書ではネットワークの記載なし	ネットワークからの渋滞情報・災害情報の取得により渋滞の緩和,災害時の避難などに役立つと考えられる	ネットワークからの最新状況の不足による事故・違反が起きる
	ネットワーク情報が最新でないか,周辺の車両からも情報を取り込み最新化されているか確認を行う	ネットワークの間違った情報による判断ミスよる事故・違反が起きる
自動運転レベル 3 報告書では検知しクラクションを鳴らす機能がない	レベル3では,クラクションによる注意喚起は自動では行われない.それを自動で行うことに的確に注意喚起を行う	通行人・他自動車へクラクションを鳴らすことにより注意・意思が伝わらず事故につながる
		通行人・他自動車へクラクションを鳴らすのが遅れたことに注意にならず事故につながる
自動運転レベル 3 報告書ではサイバーセキュリティの記載なし	レベル5では,IoTの乗っ取り,悪意あるアプリケーションのダウンロードを防ぐため必須	サイバーセキュリティが装備されていないことにより,IoT機器をのっとり,車両へ悪意のあるアプリケーションをダウンロードがされ事故・事件・盗難が起きる恐れ
	対応漏れが出ないようある程度の単位で対応を行えるようにする必要がある.	サイバーセキュリティが装備や更新が 遅すぎるとIoT機器をのっとり,車両へ悪意のあるアプリケーションをダウンロードがされ事故・事件・盗難が起きる恐れ,保安基準を満たせず責任を問われる
自動運転レベル 3 報告書では検知しパッシングの自動機能なし	レベル3では,パッシングによる注意喚起は自動では行われない.それを自動で行うことに的確に注意喚起を行う	通行人・他自動車へパッシングによる注意が伝わらず事故につながる
		遅すぎるパッシングにより通行人・他自動車への認識が間に合わず事故につながる
自動運転レベル 3 報告書では音に関わる自動機能記載なし	レベル3では存在しない遮断機,クラクション,救急車,消防車等の音を認識し,停止,端によるなどの機能追加が必要	遮断機・クラクション・救急車サイレン等が聞こえず事故につながる
自動運転レベル 3 報告書では匂いによる自動機能なし	レベル3では存在しない匂いによる故障の判別などを行える	異臭よる故障に気付かない
自動運転レベル 3 報告書では振動による自動検知機能の記載なし	レベル3では存在しない振動やハンドルによる抵抗感による車両の異常を検知する	振動による故障に気付かない 走行の安定感がない
自動運転レベル 3 報告書ではインフラ整備についての記載なし	レベル5の実現化において,認識の精度を高めるため標識の統一や横断歩道の追加,視覚の誤認識を起こしやすい道路の改修など,インフラ整備に関するルール決めが必要	インフラ整備が行われていることにより自動運転を行う上で動作が保証される
自動運転レベル 3 報告書ではネットワークの記載なし	ネットワーク情報が最新でないか,周辺の車両からも情報を取り込み最新化されているか確認を行う	ネットワーク情報のタイムラグにより最善の対応を行うことが出来ない
事故事例では,通行人は自動車を認識することが出来ていなかった	今回のケースでは,薬物が検出されており,正常な意識をもっていなかった可能性がある. そのような人物である場合は,道路に入場させない.	自動車を認識できないことにより通行人・他自動車が回避行動を行うことができない
		自動車を遅すぎる認識で,車両・身体の損失または人命の損失
事故事例では通行人が道路を横断しないという交通ルールを守らなかった	現時点は自動運転による通行人の交通ルール改正はないが,今後通行人に対するルール追加の検討の考慮が必要	交通ルールを侵害し罪に問われる

3.2.3. FRAM を用いた分析

FRAM でのモデル化において人間が運転する場合に「運転」を中心機能ととらえ，モデルを作成した.「運転」は，自車だけを制御するだけでなく，外部への制御の働きかけをすることで交通全体としての安全性を確保している事がモデルとして想起され示された．

さらに，FRAM によってモデル化することにより運転の目的を 2 つに分解する事が想起された．①目的地に早く着きたい．②目的地に安全に着きたい．前者の機能を「目的地に向かう」機能と定義し，後者の機能を「事故を回避する」機能と定義した．

「目的地に向かう」機能は，道路情報に基づき最適な経路で目的地に向かって移動する機能を提供する.「事故を回避する」機能は，外部環境から判断して事故が発生しない行動をとる機能を提供する．

次に，「目的地に向かう」「事故を回避する」機能を AI により自動化するモデルに変更した．自動運転では，「事故を回避する」機能が安全性を保証する機能として重要になる．レジリエンスエンジニアリングの観点から 4 つの機能のうち「Monitor」「Anticipate」を追加した（図 3，詳細は参考文献[10]を参照）．FRAM のモデルにおいて「事故を回避する」機能の前に「外部環境を認識する(Monitor)」機能「危険を予知する(Anticipate)」機能を追加した．特に「危険を予知する」機能が時間的制約条件（衝突までの時間）を付与するものであり重要であると言える．さらに，「事故を回避する」機能は，外部環境に対して影響を与える機能「パッシングする」「クラクションを鳴らす」へのトリガーとなる事を示している． 以上のことから，自動運転においても「危険を予知」した場合には，「パッシングする」「クラクションを鳴らす」など，外部環境に対するコミュニケーションをとる事で，交通全体としての安全性が確保できることを示している．なお，外部環境とのコミュニケーションが断絶される場合，安全性が確保できない可能性がある事を示す．

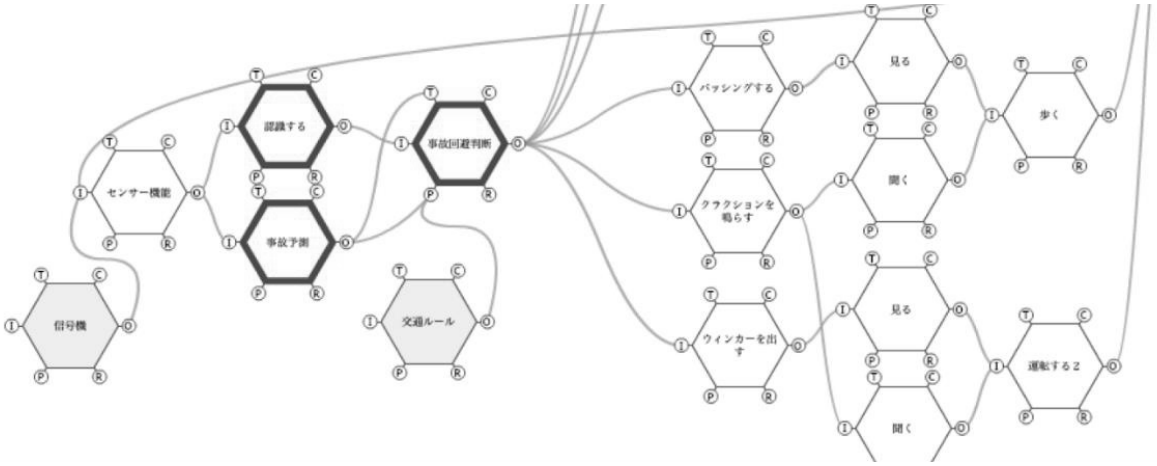


図 3：FRAM モデル

事故報告書の事故でも,「危険を予知」し,「パッシング」して確認するとともに車が通ることを相手に伝える,「クラクション」を鳴らして相手に車が通ることを伝える，という機能が存在していれば，事故を回避できた可能性があることがわかった．本分析による結果は，自動運転においても，まず相手に自車の存在を伝え，交通全体としての安全性を確保する挙動をとる事が求められていることを示している．以上のことから我々は，人が道路を横断するという想定外の事象を想定し，外部環境に対するコミュニケーションをとることで事故を回避する手段を検討する必要性があることを提言する．危険を予知して相手と意思疎通をはかりお互いに回避行動をとることで安全性向上が見込める．

3.3. 考察

CAST を用いた分析では 5 階層モデルを組み合わせることで，分析の軸や多数のヒントを得ることができ，より具体的な欠陥の導出，経時的な変化に対する欠陥の導出ができた．その結果，関連するコンポーネント（運転者，歩行者，センサー・カメラ・システムの組み合わせ等の利用される技術）の網羅・分析ができたと考える．本結果より安全性，リスクに対する評価・冗長性への配慮不足への対応に向けた強化ポイントが導出できた．

STPA を用いた分析では，従来の分析手法と違いガイドワードが経時的な内容を示しているため，想定できる事象の範囲が広がったと考え，コンポーネント間の関係性を繰り返し考慮することでハザードの抜けが発生しにくいと考えた．ゆえに自動運転レベル 5 に置き換えた際に不足している機能の洗い出しが容易になったと考えられる．また，前提条件を実際に起きた事故事例にすることと，ハザードより自動運転レベル 5 の機能を洗い出し登場人物とすることで,「それぞれの想定外」をピンポイントで抽出が出来たと考える．

FRAM を用いた分析では，人間が運転する場合の成功要因を自動運転に反映する事により，自動運転に要求される機能に対して新たな気付きが得る事ができ，レジリエンスエンジニアリングの有効性を確認できた.ツールを用いた分析は,モデル化で表現することにより，新しい発想で論理的に思考を展開できたと考える．また，モデル化のためのツールをつかうことによって思考実験を繰り返すことが可能になったと考える．

本稿における 3 つの分析を統合的に考察すると，STAMP シリーズの STPA と CAST のハザードを共通化することで 2 つの分析を連動して使うことができるのではないかと推察される．また CAST，STPA，FRAM の連動分析として，FRAM の機能はアクションであり，STAMP の CS 図における CA に相当すると考えて分析をすることで連動できると考えた.このことは，システム思考とレジリエンスエンジニアリングの統合的な活用の可能性を示すことができるのではないかと思われる．

4. 今後の課題

CAST を使い想定外を想定するためには，CAST5，6 の作業で，損失に至った不適切な制御をいかに多く抽出できるかであると考える．そのためには，できるだけ多くの利害関係者

と事実情報をより多く把握すること，及び，本来備わっているべきと考えられる安全制御をいかに多く想定できるかが課題となる．

また，自動運転レベル 5 に対応した改善勧告にするには，安全制御の想定を，現状のものから自動運転レベル 5 を考慮し発展させる必要があると考える．本実験では，自動運転レベル 5 を踏まえて検討できているかの視点では十分とは言えず，今後の課題となる．

こうした分析では繰り返しの作業が発生するためツールのサポートが必要であると考える．そのツールは，繰り返し作業や表の整理が容易に行えるものが望ましい．

自由な発想に基づく改善勧告を導出した場合には，コスト面や技術面で実現が困難となる勧告が導出される場合があるので，モデル化の際に前提条件や制約条件として考慮をすることで現実的な勧告に誘導することができるのではないかと考えられる．

セキュリティの観点での分析ができていない．物理の世界とソフトの世界の融合がされたシステムにおいては，セキュリティも検討する必要がある．

CAST 分析以外でも，作業時間を計測し，分析ツールの効率性／有効性を定量的に分析するが望まれる．

また，3.3 節で述べたようなシステム思考とレジリエンスエンジニアリングの統合的な活用を行うための具体的な方法論を構築していくことが今後の課題である．

5. まとめ

CAST と 5 階層モデルを組み合わせたことでシステム全体を広く俯瞰に捉えた改善勧告ができ，STPA ではガイドワードのサポートにより経時的な問題に関する改善勧告ができ，FRAM では成功要因に基づく新たな着眼点からの改善勧告ができた，以上によりそれぞれが想定外の改善勧告を導出することができたと結論付けた．今後，4 章で述べた課題に取り組むと共に，研究を発展させていきたい．

参考文献

[1]経済産業省，自動走行ビジネス検討会 - 報告書「自動走行の実現に向けた取組報告と方針」Version4.0，
https://www.meti.go.jp/shingikai/mono_info_service/jido_soko/20200512_report.html，2020.5.12，2021 年 1 月 8 日アクセス確認

[2]AINOW，囲碁 AI がプロ囲碁の世界に与えた影響，
https://ainow.ai/2020/11/20/246960/，2020.11.20，2021 年 1 月 8 日アクセス確認

[3]National Transportation Safety Board, Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian Tempe, Arizona March 18, NTSB/HAR-19/03 PB2019-101402, 2018, 2018.3.18

[4]独立行政法人 情報処理推進機構（IPA），はじめての STAMP/STPA ～システム思考に基づく新しい安全性解析手法～Ver.1.0，
https://www.ipa.go.jp/sec/reports/20160428.html，2021 年 1 月 8 日アクセス確認

[5]Nancy G. Leveson, Engineering a Safer World, MIT Press, 2012

[6]Kaneko, Tomoko; Yoshioka, Nobukazu; Sasaki, Ryoichi. “STAMP S&S: Safety & Security Scenario for Specification and Standard in the society of AI/IoT”, 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2020, 2020.12.11-14

[7]Hollnagel. E，社会技術システムの安全分析―FRAM ガイドブック，2013

[8]高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議，官民 ITS 構想・ロードマップ 2018，2018.6.15

[9]Nancy G. Leveson, CAST HANDBOOK: How to Learn More from Incidents and Accidents, 2019

[10] 日科技連ソフトウェア品質管理（SQiP）研究会第 36 年度研究コース 6，成果発表会付録資料，2021.2.26

[1] 経済産業省，自動走行ビジネス検討会 - 報告書「自動走行の実現に向けた取組報告と方針」Version4．0，https://www．meti．go．jp/shingikai/mono_info_service/jido_soko/20200512_report．html，2020．5．12，2021年1月8日アクセス確認

[2] AINOW，囲碁AIがプロ囲碁の世界に与えた影響，https://ainow．ai/2020/11/20/246960/，2020．11．20，2021年1月8日アクセス確認

[3] National Transportation Safety Board， Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian Tempe， Arizona March 18， NTSB/HAR-19/03 PB2019-101402， 2018，2018．3．18

[4] 独立行政法人 情報処理推進機構（IPA)，はじめての STAMP/STPA ～システム思考に基づく新しい安全性解析手法～Ver．1．0，https://www．ipa．go．jp/sec/reports/20160428．html，2021年1月8日アクセス確認

[5] Nancy G． Leveson，Engineering a Safer World， MIT Press，2012

[6] Kaneko， Tomoko；Yoshioka， Nobukazu；Sasaki， Ryoichi． “STAMP S&S：Safety & Security Scenario for Specification and Standard in the society of AI/IoT”，2020 IEEE 20th International Conference on Software Quality， Reliability and Security Companion (QRS-C)， 2020， 2020．12．11-14

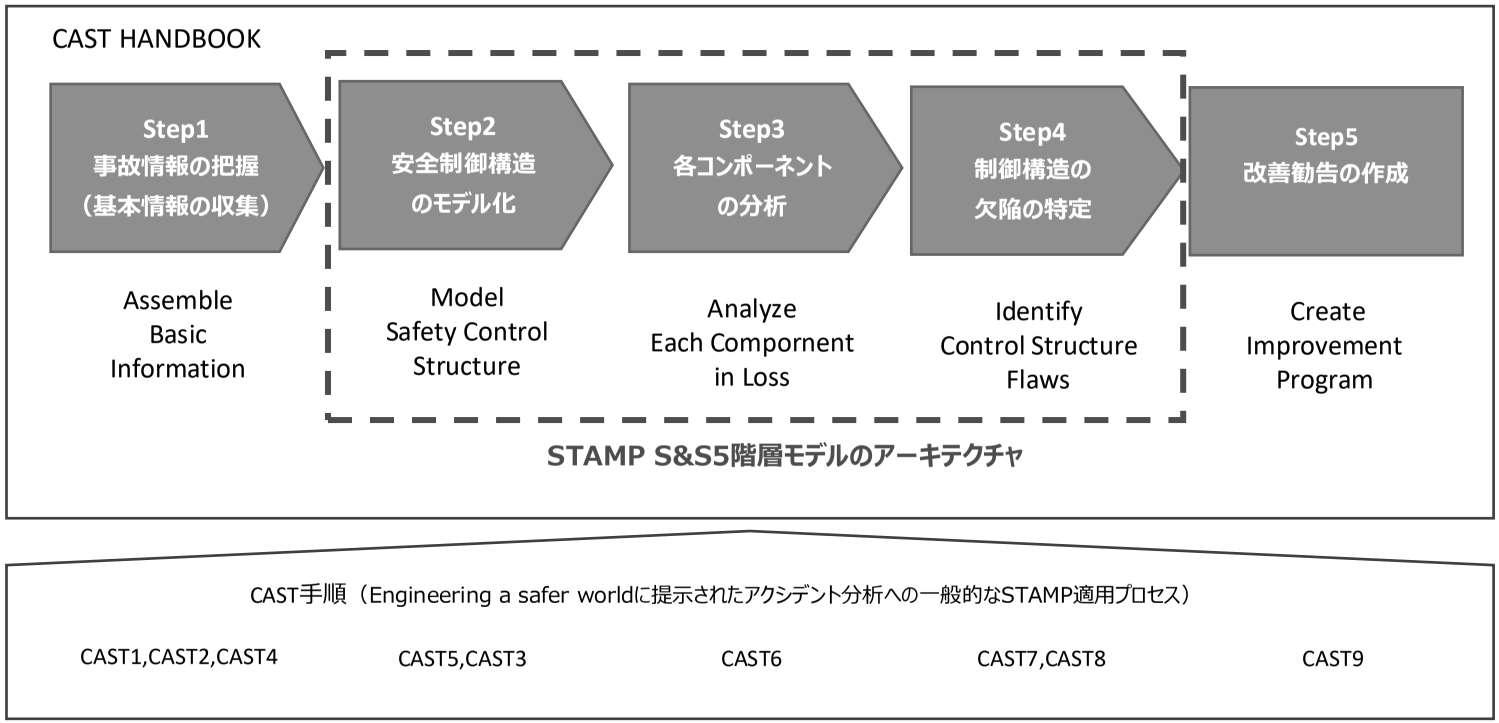
[7] Hollnagel．E， 社会技術システムの安全分析―FRAM ガイドブック， 2013

[8] 高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議，官民ITS構想・ロードマップ2018，2018．6．15

[9] Nancy G． Leveson，CAST HANDBOOK：How to Learn More from Incidents and Accidents，2019

[10] 日科技連ソフトウェア品質管理（SQiP）研究会第36年度研究コース6，成果発表会付録資料，2021．2．26

付録1_図1： CAST分析のステップ



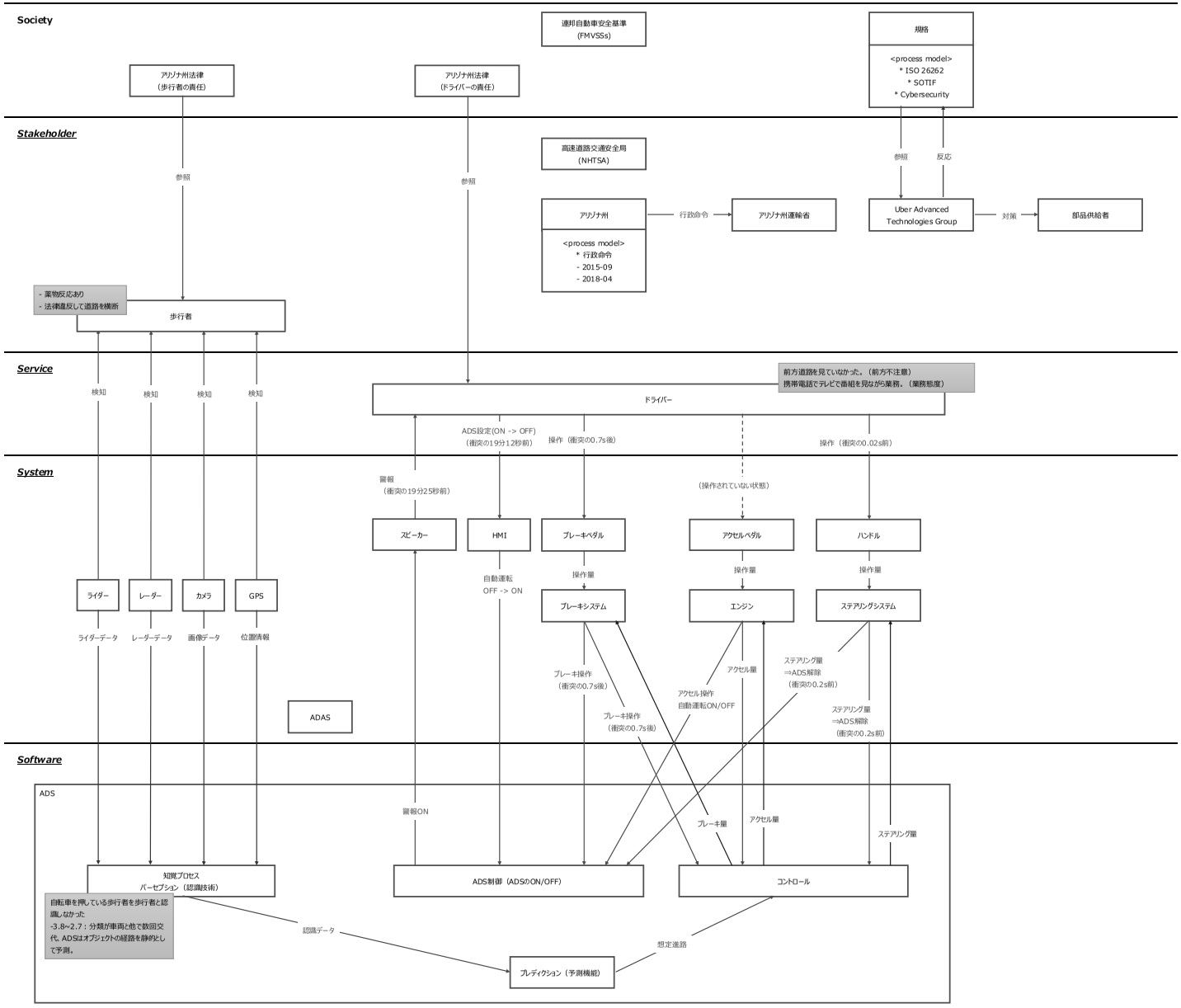
付録2_表1：アクシデント／ハザード／安全制約／イベントチェーンと質問生成結果

アクシデント（クラッシュサマリより）	ハザード（クラッシュサマリより）	安全制約	損失に近接する発生イベント（What？：何が起きたのか）	イベントが発生した理由の回答を求める質問を作成（Why？：原因究明の為明らかにしたいこと）	調査報告書による説明	各イベントが派生した理由の説明に対して、回答する必要がありそうな質問を追加
車両が歩行者に衝突された	歩行者の車道への侵入	車道に侵入させない	イレイン・ハーツバーグさん（49女性）が、自転車を押して歩行者横断禁止道路に侵入した。	なぜ歩行者は横断禁止道路に侵入できたのか？	1.2.2 中央：写真画像から、物理的なものは無し。	
				歩行者は横断禁止を認識できたか？	1.7.1 歩行者：アルコール反応無し、薬物反応あり。	正常な判断ができる状況だったか？
					1.1 クラッシュイベント：「午後9時58分」	夜間に歩行者横断禁止の標識が見えたか？ **→ 事故後、標識が追加された(1.2.2)が、そもそも夜間でも見えるようになっているかは不明。**
				歩行者侵入を物理的に防ぐものはあったか？	1.2.2 中央：写真画像から、物理的なものは無し。	歩行者が侵入できないようフェンス等を設けなかったのはなぜか？ **→　事故後、歩行に不向きな地形を作り出している(1.2.2)が、侵入はできる。**
		歩行者に法律を守らせる	歩行者が横断歩道のない場所で接近する車の前を横断、アリゾナ州法に違反する行動をしていた	なぜ法律を守らせることができなかったか？	「F6」セルと同様。 1.7.4アリゾナ歩行者と運転者の責任に関する法律 アリゾナ州法　28-793、28-794	歩行者が侵入できないようフェンス等を設けなかったのはなぜか？ **→　事故後、歩行に不向きな地形を作り出している(1.2.2)が、侵入はできる。**
		歩行者が法律を守る	〃	なぜ法律を守らなかったか？	1.1 クラッシュイベント：「午後9時58分」 1.7.1 歩行者：住所不定、活動履歴等の追加情報なし。アルコール反応無し、薬物反応あり。 1.7.4アリゾナ歩行者と運転者の責任に関する法律 アリゾナ州法　28-793、28-794	夜間に歩行者横断禁止の標識が見えたか？ **→ 事故後、標識が追加された(1.2.2)が、そもそも夜間でも見えるようになっているかは不明。**
		車道異常をドライバーに警告する	ドライバーのハンドル操作は衝突の0.02秒前、ブレーキ操作は0.7秒後(衝突後)。	道路の異変を検知しドライバーに伝える仕組みは無かったのか？	報告書記載無し	**異常な状況をおこさない、もしくは異常発生時にドライバーに警告する仕組みは必要ないか？**
歩行者が車両に衝突された	ドライバーの運転に関する力量が不足	歩行者に衝突しないよう、車両をコントロールできる	車両コントロールしていない。 2018年3月18日午後9時58分頃、アリゾナ州テンピで自動運転車の試験走行中、N.ミルアベニューの北行き車線で自転車を押して道路を横断していた女性（イレイン・ハーツバーグさん:49）をはねて死亡させる人身事故発生。車線数は左折用2車線、直進用2車線、バイク用1車線を含む計5車線。左折専用路線が分岐し始める地点で事故が発生。 横断中の女性歩行者に、2017年型ボルボXC90スポーツ多目的車（SUV）を改造した自動運転試験車両を衝突させた。	上記「車両側が歩行者を認識する」へ	-	-
			（報道されている情報より） 事故の数日前には、ある従業員が上司に対し、同車両は安全ではなく日常的に事故を起こしている、として車両制御者の訓練について懸念を示していた。	事故の記録はなかったのか？	1.7.2 ドライバー：雇用中の処罰記録なし	「Uberの安全文化・方針浸透が不十分」へ
				ドライバーの運転に関する力量が不足していたのか？	**1.8.1　CFR（連邦規則集）390.5の下では、このような車両は商用自動車の定義を満たさず、したがって、それらを操作する人々は商用運転免許を必要としなかった。**	「州がADS試験の安全を監督していない」へ
				アリゾナ州の法律は、ATG車両の運転者が商業運転免許を取得することを要求していなかった	1.8.1　アリゾナ州法では、UberまたはATGが提供する輸送サービスは、タクシー、ライブラリー、またはリムジン運行に分類されておらず、むしろ「輸送ネットワーク会社」として分類されていた。（中略）	「州がADS試験の安全を監督していない」へ
				訓練は十分だったか？	1.8.3　以下の資格を満たした候補者のみが、車両運転者訓練プログラムのために考慮された:(1)少なくとも21歳;(2)年齢に応じて最低1〜3年の運転経験;(3)過去3年間の3つ以下の軽微な運転違反;(4)過去3年間の重大な交通違反;(5)過去7年間の重大な交通違反 1.7.2.1　**2017年6月からATGの自動運転事業者**として働いていた 1.7.2　ATG記録：オペレータは、3週間の訓練プログラムおよびその後の反復訓練クラスを完了（※アリゾナ自動車の記録：衝突の10年前には、車両運転者は4つの交通違反を有しており、そのうちの最後は2016年4月であり、スピードアップのためであった。（中略）報告可能な衝突はなかった。（補記：ドライバーは車両運転者訓練プログラム受講対象者として、プログラムを受けていたと解釈）） ATGの方針、手続き、会社の価値観に焦点を当てた3日間の教室訓練と、試験車両および手動車両操作のダイナミクスに精通した2日間の教室訓練	なし
	Uberの安全文化・方針浸透が不十分	安全文化・方針が定められ、浸透・遵守している	浸透していない	なぜ浸透していない？	1.8.2：ATGの自動車運転者に対する安全に関する方針あり 1.8.2：ATGは、ADSを公道でテストするリスクを評価する責任のみを負う、企業の安全部門や専任の安全管理者を持たず、作業長が安全管理者の任務を負った。（安全管理者の代表的な業務には、安全説明会の実施、運転上のリスクと損失防止の評価、安全文化の維持を含むが、ATGは、スポット確認の頻度を記録することはできなかった）	-
				事故を起こしたドライバーは認識していたか？	1.8.2 ・ATGの自動車運転者に対する安全に関する方針あり ((1)携帯電話の使用およびテキストの不使用、(2)シートベルトの使用の義務化、(3)薬物検査－雇用前、ランダム、合理的な疑い、および事故後、(4)最大10時間の運転時間、(5)運転者資格の専門的な行動および維持) ・ATGは、全体的なジョブパフォーマンスに基づく報酬プログラムを有していた ・ATGは違反に対する段階的な(3段階の)懲戒プログラムを有していた（薬物、運転中の電話など、人々を危険にさらす違反） ・64 (a) 携帯電話のポリシーは、訓練の最初の1週間の間、車両オペレータとレビューされた。また、オペレータに提供する方針書にも記載した。ただし、従業員は、携帯電話の使用に特化した方針のコピーに署名したり、受け取ったりしなかった	-
			遵守されていない	事故を起こしたドライバー含め、違反者が適切に抽出されていたのか？	＜抽出の仕組み＞ 1.8.2 ・ATGは衝突時に薬物検査の方針を設けていたが、散発的に実施 ・ATGは、車両オペレータに、ATGポリシーの違反を**自己報告**し、**ピアによる違反を報告**することを奨励した ・ターミナル・マネージャーは、内向きカメラからのビデオを**無作為**に調べて、車両オペレータが会社の方針を遵守しているかどうかを**スポット・チェック** **・スポットチェックは頻繁ではなく、通常、起こり得る違反が報告された後にのみ起こった** ＜抽出状況＞ ●Uber全体 1.8.2NTSBの捜査官に提供された資料によれば、2017年4月から2018年2月にかけて、内向きカメラの動画を調査した結果、ATGは同社の携帯電話ポリシーに違反した車両運行会社18社を特定した。9名が修復訓練を受け、9名が終了した ●事故を起こしたドライバー 治験責任医師は、ATGが、Tempe衝突前に、衝突に関与した車両運転者のビデオ記録を調べたという証拠を見つけなかった。同僚からの報告はなく、就職中に懲戒処分を受けなかった。インタビューを受けたとき、彼女の上司はオペレータのビデオをレビューすることを報告しなかった。	-
			違反行為が抽出されていない	なぜ、事故時点で違反行為が抽出されなかった？	●事故を起こしたドライバー（同上） 1.8.4 単体オペレーターへの移行 事故を起こしたドライバーが訓練開始時、ATGプロトコルは、ADS操作中に試験車両に2人を必要とした。 ・1人は運転席を占有し、引き継ぎの可能性に備えて環境を監視 ・第2のオペレータ「イベントタグ付け」は、前部乗客席を占有。タグ付け装置は、ラップトップを使用し車両の経路を監視、関心のある任意の状況(予期しないADSアクションまたは環境内の異常なイベントなど)に注釈をつけた ⇒ATGは、2017年9〜10月、車両運行会社2社の責任を単一運行会社に集約。HMIタブレットを備えた試験媒体を装備。ADSとの単純操作。単一オペレータへの移行は、ATGが試験車両の数を増やすための運用上の決定。 （HMIタブレットは、単一オペレータが運転監視およびタグ付けタスクの両方を実行できるようにタグ付けタスク単純化のため） Tempe衝突の車両運転者は、イベントタガーとして訓練、2017年10月25日、一次/単独オペレーターに切り替え 1.9.2.2車両運転者の監督(※事故後の改善)	-
		安全文化・方針を遵守させている		遵守させるようになっていたのか？	＜浸透の仕組み＞同上 ＜違反者抽出の仕組み＞ 1.8.2 ・ATGは衝突時に薬物検査の方針を設けていたが、散発的に実施 ・ATGは、車両オペレータに、ATGポリシーの違反を**自己報告**し、**ピアによる違反を報告**することを奨励した ・ターミナル・マネージャーは、内向きカメラからのビデオを**無作為**に調べて、車両オペレータが会社の方針を遵守しているかどうかを**スポット・チェック** **・スポットチェックは頻繁ではなく、通常、起こり得る違反が報告された後にのみ起こった** 64 (a) 携帯電話のポリシーは、訓練の最初の1週間の間、車両オペレータとレビューされた。また、オペレータに提供する方針書にも記載した。ただし、従業員は、携帯電話の使用に特化した方針のコピーに署名したり、受け取ったりしなかった	-
	州がADS試験の安全を監督していない	州がADSの安全を監督する	ADOT（アリゾナ運輸省）に対し、ATGは自動運転車であることを確認する書面を提出していない。	なぜ提出していなかったのか？	アリゾナ州では、自動車の試験に対する要求が限られており、アリゾナ州にADS試験の安全リスクに対応への承認プロセスがない	-
					1.10.2 ・州内の自動車の操作はExictiveOrder2015-09で規制 人が車内にいたかどうかにかかわらず自動車の試験と運転を許可 車両の内側または外側の人が必要に応じて車両の移動を指示すべきということ。自動車の試験のためのアプリケーションの要求をADOTに指示しなかった ・執行命令2018-04のADS搭載車が州内で使用できるパラメータを承認。主なパラメータは車内かどうかであった （ADS搭載車両を内部に搭載して試験または運用する開発者は、すべての連邦法、アリゾナ州法、アリゾナ改正法第28号、アリゾナ運輸省が定めるすべての規制および方針に従うことを、執行命令によって求められる） 注文には、**少なくとも一人の人物が占有する自動車に関する他の安全に焦点を当てた要件は含まれていない。**無人ADS搭載車を試験する開発者(車内に人がいない場合)は、ADOTに対し、自動車であることを確認する書面を提出する必要がある。（中略）執行命令2018-04では、ADS試験を実施する事業体が車両内のオペレータとの適合性を確認する声明を要求していないため、ATGはADOTに提出しなかった。 **⇒車内にADSを搭載or無人ADS搭載車のみで、人が占有する自動車に関する他の安全に焦点はあてられていない**	-
					・アリゾナ運輸省の自動車両試験の不十分な監督 ・安全勧告H-19-49：開発者は衝突またはオペレータの不注意に関するリスクを管理する計画を提出し衝突を防止、またはADS試験パラメータ内の衝突の重大性を軽減するための対策を確立する、ADS装備車両の試験のためのアプリケーションを提出する必要がある ・安全勧告H-19-50：ADS装備車両を試験するためのアプリケーションを評価する専門家のタスクグループを設置し、その後試験許可を付与する	-
					2.3.4.1カリフォルニア州 2.3.4.2ペンシルベニア州 では、事故後に規制強化等の対応をとっているが、アリゾナ州は事故後でも規制強化を行っていない(2.3.4.3)	-
	高速道路交通安全局NHTSAに、自動運転車を公道で走行させる安全リスク管理要件がない	自動運転車に関する安全リスク管理要件がある	・高速道路交通安全局に、自動運転車両政策にADSを評価する手段がない ・1.10.1本報告書の日付現在（<--？？いつのこと？）、FCW,AEB,ADSなどのシステムに必要な安全基準を策定しておらず、最小ADS性能を評価するための試験手順を提案していない ・2016年9月に、自動車に関する初期方針文書を公表（ADS搭載車両の試験及び配備に関する基本的な指針を示した）。また、車両内部にオペレータを持つための要件によって作成された自律的な車両使用に対する障害物の除去に焦点を当てたモデル状態方針を提案 ・第1の政策：開発者に安全性自己評価報告書を機関に提出するよう求めるプロセスの計画を概説。（自主的、将来的に義務付けられるかもしれない） ・第2次自動車政策2017.9 12の安全要素を記載、安全自己評価報告書の作成に使用するために製造業者などに要約ガイダンスを提供 開発者は各要素の目標を達成するためのプロセスを作成することを奨励 **⇒開発者がどのようにこれらの目標を達成すべきかの具体的な情報はほとんど得られなかった。また、開発者やほかの人々に、自分たちの安全プロセスを評価する手段を提供しなかった** **この方針は、自動車の開発時に開発者がガイダンスを遵守すること、または安全性自己評価報告書を提出することを要求しなかった。この方針は、評価報告書が提出された場合、NHTSAの承認を受けなかった**		★・安全勧告H-19-47：公道で開発用自動運転システムを試験する団体に安全性自己評価報告書を提出するよう要求する ・安全勧告H-19-48：H-19-47に要求される安全自己評価報告書の継続的な評価のためのプロセスを確立し該当する場合には、車両運転者の関与の適切な監視を含む、行動上の開発自動運転システムを試験する適切な保障措置が計画に含まれているかどうかを決定する (事故後) 2018年10月、NHTSAは3番目の自動車両政策(NHTSA 2018)をリリース。この文書は、同機関のガイダンスを、米国運輸省の他のモーダル機関にもわずかに拡大。第3版は、自動化-SAEレベル3、4、5.81のレベルが高い車両に焦点を当てている。第2および第3の政策は、自動化システムに悪影響を及ぼす可能性のある技術中立システムおよび法律に焦点を当て、ADSに関する州および地方政府のベストプラクティスおよび勧告を概説。第3版では、試験自動車の運転者に対する実施要件を検討するよう州政府に提案したが、具体的な事例は示さなかった。 117　NHTSAのAutomated Driving Systems 2.0ポリシーは、「ADSに関連する国家の役割と活動を支援するために、政府レベルでの新しい監督活動」を検討することを国家に提案している。NHTSAは、「ADS活動を支援するために、国家が特定の新しいエンティティを作る必要はないと予想している」と続けている。	-
	米国自動車管理協会が自動運転車の安全に対する対策に関与していない	自動車管理協会が自動運転車の安全対策にも関与する	安全性自己評価報告書が自主的な提出である		安全勧告H-19-51： ★州に連絡し ・開発者にリスク管理の計画をして対策している計画を求め、評価するタスクグループを設置するよう奨励する	-
	連邦にADS試験に関する安全基準や審査の仕組みがない	連邦で統一されたADS試験に関する安全基準がある	連邦に自動運転システムとすべての州の道路交通安全のための安全基準、評価プロトコルがない		2.3.4.4 「NTSBは、ADSの連邦安全基準および評価プロトコルが欠如していること、ならびに NHTSAの安全性自己評価プロセスが不十分であることを考慮すると〜」 連邦安全基準と評価プロトコルの欠如について記載 117　NHTSAのAutomated Driving Systems 2.0ポリシーは、「ADSに関連する国家の役割と活動を支援するために、政府レベルでの新しい監督活動」を検討することを国家に提案している。NHTSAは、「ADS活動を支援するために、国家が特定の新しいエンティティを作る必要はないと予想している」と続けている。	-
	車両側が歩行者を認識できない	車両側が歩行者を認識する	ドライバーが事故直前まで歩行者を認識していなかった。	なぜ歩行者を認識できなかったのか？	1.1 クラッシュイベント：ドライバーは長時間、車道から目を離し、携帯電話を置いた中央コンソールの底部見降ろしていた。 1.7.2 ドライバー：午後9時16分から午後9時59分までの間にテレビ番組を継続的にストリーミングしていた記録あり。 追加情報：セーフティドライバーのラファエル・ヴァスケス被告は、事故当時、テレビ番組「The Voie」を視聴しており、前方道路を見ていなかった。動画配信サービスHulu側にも、ヴァスケス被告が事故当時、テレビ番組をストリーミングしていた記録が残っているとみられる。携帯電話でテレビ番組を視聴しながら業務に当たっていた。	「Uberの安全文化・方針浸透が不十分」へ ドライバー個人についてはCAST5-1以降へ
				自動運転でドライバーは前方注意義務が無かったのか？	1.8.2 安全文化・方針：ドライバーは携帯電話使用等のポリシーに対して署名しなかった。	「Uberの安全文化・方針浸透が不十分」へ ドライバー個人についてはCAST5-1以降へ
			自動運転システムが正しく作動しなかった。	自動運転システムは、歩行者を認識しなかったのか？	下記、システム側へ	
歩行者との衝突が発生した	自動運転システムが歩行者を認識しない	自動運転システムが歩行者を認識しなければならない	(-5.6) レーダーは、歩行者(車両として分類)の最初の検出を行い、速度を推定する。	Q1：なぜ、レーダーは歩行者を車両に分類したのか？	A1-1. 横断歩道のない場所でN.ミルアベニューを横断していたため、システムは彼女を歩行者として分類しなかった(1.5.6.1) A1-2. システムの設計には信号無視の歩行者への配慮が含まれていませんでした。(1.5.6.1)	Q1-1. なぜ、横断歩道のない場所を横断した場合、歩行者と判断しないのか？ Q1-2. 歩行者と判断する条件は何か？
				Q2：速度は正しく推定できたのか？	A2-1. 詳細な記述無し	-
				Q3：カメラはどのような分析をしていたのか？	A3-1. 衝突の約2秒前に歩行者が見えるようになっています。それ以外の部分の詳細は、ヤヌス前方カメラの映像と一致しています。(1.5.6.2)	Q3-1. なぜ、衝突の2秒前まで見えなかったのか？
				Q4：ライダーはどのような分析をしていたのか？	A4-1. 詳細な記述無し	-
				Q5：カメラとライダーの分析結果は考慮されていたのか？	A5-1. 3 つのセンサーシステムの融合を利用して、検出された物体を分類している。ADS では、特定の感覚系による追跡を他の感覚系よりも優先させる優先順位付けスキーマを使用していたが、これは観測の頻度にも依存していた。(1.5.5.1) より最近に検出された物体は、ADS 分類スキーマでより高いトラッキング優先度を受けました。(補足31)	-
			(-5.2) ライダーは未知の物体を検出する。 オブジェクトは新しいと見なされ、追跡履歴は利用できず、速度は決定できない。ADSは、オブジェクトの経路を静的として予測する。	Q1：なぜ、ライダは歩行者を未知の物体として検出したのか？	A1-1. 詳細な記述無し	-
				Q2：なぜ追跡履歴が利用できないのか？	A2-1. ステムの設計上、存在しない物体（分類を変更したもの）の追跡履歴を除外している(1.5.6.1)	-
				Q3：なぜ、速度は決定できないのか？	A3-1. 特定のオブジェクトの分類（「その他」）にはゴールが割り当てられていませんでした。現在検出されている位置は静的なものとみなされ、その位置が試験車両の進路上に直接ある場合を除き、その物体は障害物とはみなされませんでした。(1.5.5.2)	Q3-1. なぜ、その他にはゴールが割り当てられなかったのか？
				Q4：なぜ、ADSはオブジェクトの経路を静的と予測したのか？	A4-1. 特定のオブジェクトの分類（「その他」）にはゴールが割り当てられていませんでした。現在検出されている位置は静的なものとみなされ、その位置が試験車両の進路上に直接ある場合を除き、その物体は障害物とはみなされませんでした。	-
			(-4.2) ライダは、検出された物体を車両として分類し、これは、物体の変更された分類であり、追跡履歴はない。ADSは、オブジェクトの経路を静的として予測する。	Q1：なぜ、ライダは歩行者を車両として分類したのか？	（上述） A1-1. 横断歩道のない場所でN.ミルアベニューを横断していたため、システムは彼女を歩行者として分類しなかった(1.5.6.1) A1-2. システムの設計には信号無視の歩行者への配慮が含まれていませんでした。(1.5.6.1)	（上述） Q1-1. なぜ、横断歩道のない場所を横断した場合、歩行者と判断しないのか？ Q1-2. 歩行者と判断する条件は何か？
				Q2：物体の変更された分類は、なぜ追跡履歴が利用できないのか？	上述	-
				Q3：ADSはオブジェクトの経路を静的と予測したのか？	上述	-
			(-3.9c) ライダーは分類媒体を保持する。 追跡履歴および割り当てられた目標に基づいて、ADSは、左スルーレーンを移動するオブジェクトの経路を予測する。	質問なしか？	分類:自動車別ライダー 経路予測:左スルーレーン(SUVの隣);SUVの経路上ではない。	-
			(-3.8〜-2.7) 物体の分類は、車両とその他の間で数回交互に変化する。その都度、追跡履歴は利用できないため、ADS は対象物の進路を静的なものとして予測する。検出された物体の分類が変わらない場合、ADS は左車線を走行していると予測する。	Q1. なぜ、物体の分類が車両とその他で数回変化したのか？	A1-1. 詳細な記述無し	-
				Q2. なぜ、検出された物体が変らない場合、左車線を走行していると予測したのか？	A2-1. 新しい軌跡を生成する際にその物体の追跡履歴を考慮しなくなった。(1.5.5.2) A2-1. 走行車線で検出され、車両として分類された物体には、一般的にその車線の交通方向への走行目標が割り当てられる。(1.5.5.2)	-
			(-2.6) ライダーは、検出された物体を自転車として分類し、これは物体の変更された分類であり、物体は追跡履歴がない。 ADSは、自転車の進路を静的と予測する。	Q1：なぜ、ライダは歩行者を自転車として分類したのか？	（上述） A1-1. 横断歩道のない場所でN.ミルアベニューを横断していたため、システムは彼女を歩行者として分類しなかった(1.5.6.1) A1-2. システムの設計には信号無視の歩行者への配慮が含まれていませんでした。(1.5.6.1)	（上述） Q1-1. なぜ、横断歩道のない場所を横断した場合、歩行者と判断しないのか？ Q1-2. 歩行者と判断する条件は何か？
				Q2：物体の変更された分類は、なぜ追跡履歴が利用できないのか？	上述	-
				Q3：ADSはオブジェクトの経路を静的と予測したのか？	上述	-
			(-2.5) ライダーは、自転車分類を保持し、追跡履歴および割り当てられた目標に基づいて、ADSは、自転車の経路を、車線を左に通る走行として予測する。	質問なしか？	分類:自転車別ライダー 経路予測:左スルーレーン(SUVの隣);SUVの経路上ではない。	-
			(-1.5) - ライダーは未知のオブジェクトを検出します。これは未知のオブジェクトであるため、追跡履歴がなく、ゴールが割り当てられません。ADSは、オブジェクトの経路を静的として予測する。 -検出された物体は部分的にSUVの走行レーンにあるが、ADSは、物体の周りの運動計画(物体の右への操縦)を生成し、運動計画は、次の2つのデータ点について、有効な回避物体のままである。	Q1：なぜ、ライダーは歩行者を未知のオブジェクトとして検出したのか？	上述	-
				Q2：未知のオブジェクトであるため追跡履歴がなくゴールが割り当てられなかったのか？	上述	-
				Q3：なぜ、回避できると判断したのか？	**直接関係しているか分からないが・・・** 特定のオブジェクトの分類（「その他」）にはゴールが割り当てられていませんでした。現在検出されている位置は静的なものとみなされ、その位置が試験車両の進路上に直接ある場合を除き、その物体は障害物とはみなされませんでした。(1.5.5.2)	-
			(-1.2) - ライダーは、自転車を検出する;これは、変更された分類であり、追跡履歴がないが、ゴールが割り当てられる。ADSは、自転車がSUVの経路上にあると予測している。 - 自転車の周りを操縦するためのADSモーションプラン(0.3秒前に生成)ができなくなり、状況が危険(緊急事態)になる。 - 行動抑制が始まる。	Q1：なぜ、ライダーは歩行者を自転車として検出したのか？	A-1： ADSは、歩行者の分類を車両、自転車、その他と交互に数回変更した。(1.5.6.1)	-
				Q2：物体の変更された分類は、なぜ追跡履歴が利用できないがゴールが割り当てられるのか？	A-1： システムは、歩行者をそのように分類することは決してなく、システムの設計は、持続しない物体(分類が変更された物体)についての追跡履歴を除外したので、歩行者の経路を正しく予測することができなかった。(1.5.6.1)	-
				Q3：なぜもっと早く検出できなかったのか？	A-1： 夜間の状況、並びに解像度及びカメラレンズの品質のために、Janus前向きカメラからの記録は、衝突時に車両運転者が見ていた可能性のあるものを正確に描写することができそうにない。(1.5.6.2)	-
			(0.0) 衝突発生	-	-	-
			(0.7) 車両の運転者がブレーキをかける。	-	-	-
			衝突の1.2秒前に歩行者との衝突が迫っていると判断し、緊急事態を検知しました。	-	-	-
	緊急時に衝突を回避しない	緊急時には衝突を回避をする	(-1.2) - 自転車の周りを操縦するためのADSモーションプラン(0.3秒前に生成)ができなくなり、状況が危険(緊急事態)になる。 歩行者との衝突が迫っていると判断し、緊急事態を検知しました。 - 行動抑制が始まる。	Q1. なぜ、ブレーキをかけなかったのか？ (このタイミングで行動抑制をし始めたのか？)	A1-1. 危険な状況を検知した後、衝突を防ぐために0.71g以上の急制動が必要な場合には、1秒間制動を抑制するようにADSを設計していました(2.2.1.1) A1-2. 状況が衝突回避のための ADS の応答設計仕様（衝突を回避するためには 0.71g 以上の減速が必要）を超えていたため、緊急制動が抑制された(2.2.1.1) A1-3. (1)システムが検出したハザードの性質を確認して代替経路を計算するか、(2)車両の運転者が車両を制御する間、ADS が制動を抑制する 1 秒間であった。(1.5.5.3)	-
				Q2. 危険な状態をドライバーには通知したのか？	A-1： 突然の係合解除時に、システムは、オペレータに聴覚警告を送る。(1.5.4.2)	-
				Q3. なぜ、ハンドル操作による回避をしなかったのか？	A-1： 衝突のほぼ3分前に、車両運転者は、異なる時間にセンターコンソール23の底部を見た。7回の視線は少なくとも3秒間続き、最長の視線は6.9秒間続く。操作者は、打撃の6秒前に中央コンソールの底部に向かって下に向かって視線を下ろし始め、そこで、彼女は、次の5秒間、彼女の注視を保持した。彼女は衝突の約1秒前に道路に視線を戻した(1.5.6.2)	-
			それまでの移動履歴を考慮していない(1.5.5.2)	Q4. なぜ、考慮しなかったのか	A-1： ADSは歩行者の分類を数回変え、車両、自転車、その他の間を交互にした。システムは、歩行者をそのように分類することは決してなく、システムの設計は、持続しない物体(分類が変更された物体)についての追跡履歴を除外したので、歩行者の経路を正しく予測することができなかった。(1.5.6.1)	-
			アクションサプレッションが開始された際に、オペレータにアラートは表示されなかった。(1.5.5.3)	Q1. なぜ、オペレータにアラートを表示しなかったのか？	A1-1. 誤報（危険な状況が存在しないのにADSが危険な状況を認識してしまうことで、車両が不必要に過激な操作を行う原因となる）を懸念した(1.5.5.3)	-
			最大許容制動で衝突を回避できなかった場合には、車両の運転者に音声で警告すると同時に、車両の徐行を開始するように設計されていた。(1.5.5.3)	Q1. 警告はオペレータに聞こえていたのか？	A1-1.アクション抑制が開始されたとき、オペレータに警告は与えられなかった。ATGは、誤警報-ADS-に対する懸念のため、行動抑制を実施したと述べた。(P13) A1-2.最大許容制動の適用で衝突を避けることができなかった場合、システムは、徐々に車両の減速を同時に開始しながら、車両運転者に聴覚的警告を送るように設計された。(P14) A1-3.ATGは、オペレータの注意力のリアルタイム監視を可能にする新しい内向きカメラシステムを設置した。システムは、運転席の運転者が数秒間道路から注視したことを検出すると、直ちに車両の運転者に警告を送り、記録を見直す監督者に報告を送る。(P46)	-
				Q2. なぜ、オペレーターはブレーキをかけなかったのか？	A2-1. 衝突の6秒前からセンターコンソールの下の方を見始め、その後5秒間は視線を保っていました。その後、衝突の約1秒前に視線を道路に戻した。(1.5.6.2)	Q1-1. 気づくのが遅かったからブレーキをかけなかったのか？
				Q3. なぜ、オペレーターはハンドル操作をしなかったのか？	A3-1. 衝突の6秒前からセンターコンソールの下の方を見始め、その後5秒間は視線を保っていました。その後、衝突の約1秒前に視線を道路に戻した。(1.5.6.2)	Q1-1. 気づくのが遅かったからハンドル操作をしなかったのか？
				Q4. 車両は徐行したのか？	A4-1.システムは、緊急ブレーキをかけず、代わりに、車両を徐々に減速させる計画を開始したときに、車両運転者に聴覚警報を鳴らした。(P18) A4-2.車は交差点に近づきつつあり、システムは右転換を計画していたため、徐々に減速していた。(P1)	-
			最大許容制動で衝突を回避できない場合、ＡＤＳは、衝突の重大性を軽減するためだけに最大制動を適用するようには設計されていなかった。(1.5.5.3)	Q1. なぜ最大抑制を適用する設計になっていなかったのか？	A1-1.ADSは最大自動ブレーキを0.71gに制限したが、最適な路面摩擦を持つ車両の最大制動能力は1gであった。TPDは、車両の能力と路面摩擦に基づいて、衝突地帯でSUVが平均0.92gで減速できることを決定した。(P13の注記33より) A1-2.事故以降、ATGは、緊急事態においてADSが応答する方法を変更した。システムは、衝突軽減のためにも最大許容ブレーキを作動させる(1.9節参照)。(P14)	-
			衝突時にはボルボのADASは作動していなかった(1.6.1)	Q1. なぜ、ボルボのADASが作動していなかったのか？	A1-1. ATGがATG ADSの運転中にボルボのADASを解除した(1.6.1)	-
			ATGがATG ADSの運転中にボルボのADASを解除した(1.6.1)	Q1. なぜ、ボルボのADASを解除したのか？	A1-1. ボルボADASとATG ADSの同時作動は、(1) ボルボとATGシステムのレーダーは同じ周波数で作動するため、信号が誤解釈される可能性が高いこと、 A1-2.(2) SUVのブレーキモジュールは、ボルボAEBとATG ADSの両方からブレーキコマンドを受信する場合に優先順位を割り当てるように設計されていなかったことから、互換性がないと考えられていた。(1.6.3)	Q1-1. なぜ、同じ周波数のレーダーを使用したのか？ Q1-2. なぜ、優先順位を割り当てなかったのか？
			(-0.2) - アクション抑制は、それが始まってから1秒後に終了する。 - 状況は依然として危険であり、ADSは緩やかな車両減速計画を開始する。 - 聴覚的警告は、ADSが関与しており、制御された減速を開始していることを示す。	Q1：なぜ、行動抑制に1秒必要だったのか？	(1)システムが検出したハザードの性質を確認して代替経路を計算するか、(2)車両の運転者が車両を制御する間、ADS が制動を抑制する 1 秒間であった。(1.5.5.3)	-
			(-1.2 ？？) 衝突を防止するには、ADSの設計仕様を超えたブレーキが依然として必要であった。 その設計によれば、システムは、緊急ブレーキをかけず、代わりに、車両を徐々に減速させる計画を開始したときに、車両運転者に聴覚警報を鳴らした。(1.5.6.1)	Q1：聴覚警報のタイミングは適切だったのか？	報告書に記載なし ＜補足情報＞ HMIデータは、クラッシュの直前に、HMIがいかなる警報も提示しておらず、タグが入力されておらず、オペレータがクラッシュの前にHMIと対話していなかったことを示している。(P43)	-
				Q2：減速計画を開始したときに警報は鳴らしたのか？	報告書に記載なし ＜補足情報＞ システムは、徐々に車両の減速を同時に開始しながら、車両運転者に聴覚的警告を送るように設計された。(P14)	-

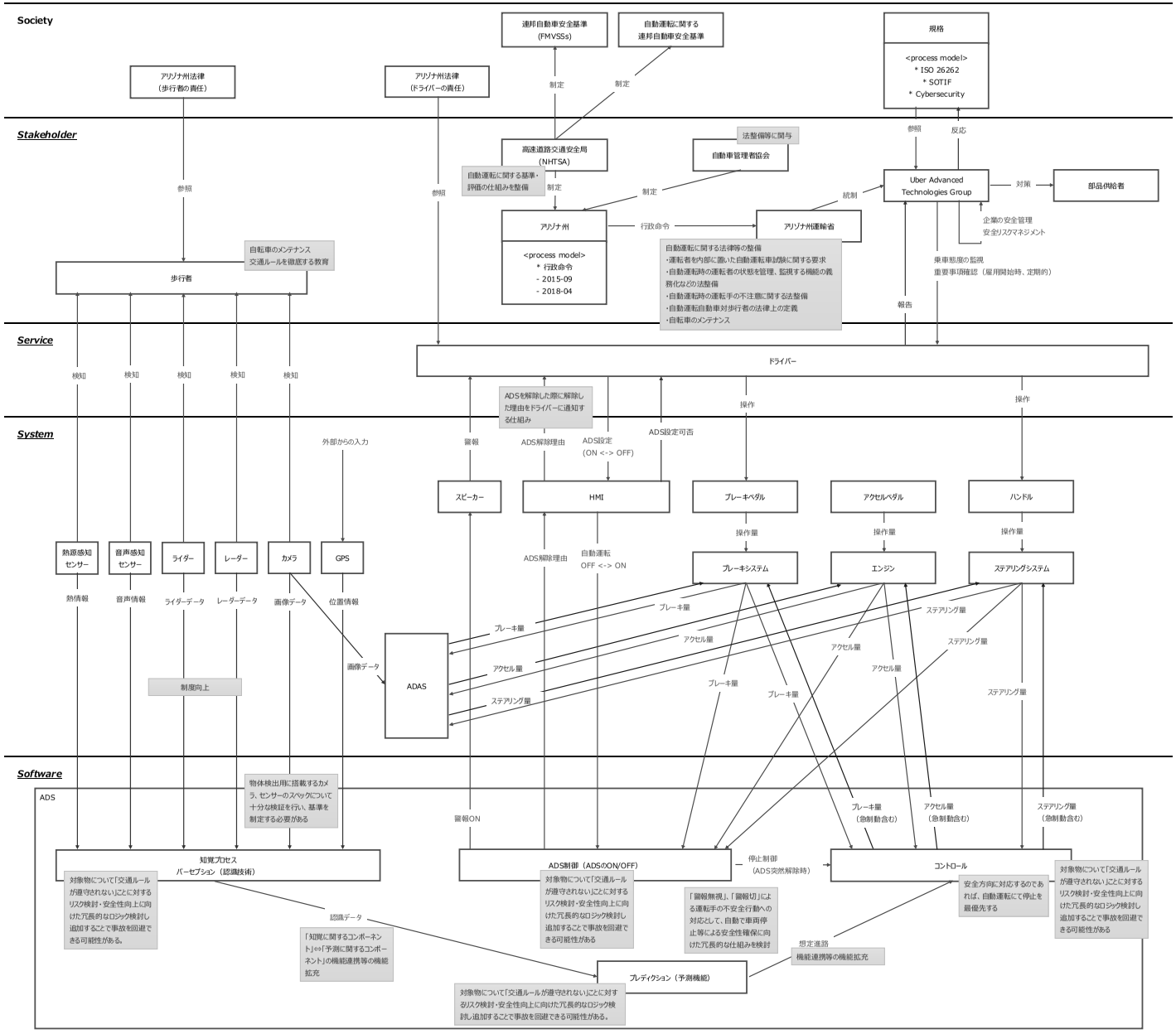
付録3_表2：具体的コンポーネントレベルでの分析結果

No	カテゴリ5階層をイメージ	事故発生対象	CAST5-1 安全上の責務(責任)	CAST5-2 非安全なコントロールアクション (CS図の赤矢印をイメージ)	CAST5-3 プロセスメンタルモデルの欠陥	CAST5-4 意思決定された状況・背景
A2	System	カメラ、センサ	・カメラ以外に検知する方法がなかったのか？ ・捉えた映像を正確に知覚プロセスに渡すこと。	ーーー カメラの映像について正確に知覚プロセスに渡すことについては報告書に記載がないため振り下げられないことより、ここまでとした。	ーーー	ーーー
A5	Software	知覚プロセス パーセプション（認識技術）	歩行者を正しく歩行者として分類する カメラ、ライダー、レーダーの情報から対象物を正しく識別する	・歩行者を正しく歩行者として分類されなかった ・信号無視の歩行者を歩行者として認識しなかった ・歩行者は横断歩道のない場所を横断していた	A1-2. システムの設計には信号無視の歩行者への配慮が含まれていませんでした。(1.5.6.1) 横断歩道付近以外の歩行者についても、明示的なゴールは設定されていなかった。(1.5.5.2)	・歩行者は車道を渡ってはならない（アリゾナ州） ・横断歩道以外の場所で車道を横断する場合は車道を走行する全ての車両に道を譲らなければならない（1.7.4）
A12	Software	知覚プロセス パーセプション（認識技術）	歩行者を正しく歩行者として分類する	ADSは、歩行者の分類を車両、自転車、その他と交互に数回変更した。歩行者をそのように分類したことはなかった。(1.5.6.1)	持続しない物体(分類が変更された物体)についての追跡履歴を除外したので、歩行者の経路を正しく予測することができなかった。(1.5.6.1)	・歩行者は車道を渡ってはならない（アリゾナ州） ・横断歩道以外の場所で車道を横断する場合は車道を走行する全ての車両に道を譲らなければならない（1.7.4）
A13	System	カメラ、センサ	・捉えた映像を正確に知覚プロセスに渡すこと。 （運転手が見ている状況と同じ情報が取得できること）	技術の状況、並びに解像度及びカメラレンズの品質に依存した状況であった。(1.5.6.2)	ーーー	・新しく販売された自転車は、前部、後部、およびペダルに反射器を有し、車輪の側壁または車輪スポークに側面反射器を有することを要求されていた。 ・車輪スポークに側面反射器を有したものを自転車と設計していた？ ・自転車のライトが地面に垂直に照らさせていたから自転車として認識しなかった？
A17	Software	予測プロセス　プレディクション（予測機能）	歩行者の移動速度が推定できること （歩行者は動いているのか？静止していたか？） 追跡履歴に基づいて、可能性のある軌跡（経路予測）を生成する(1.5.5.2) 進路を継続的に更新する(1.5.5.2)	・歩行者の移動方向を正しく認識しなかった ・対象物の切り替え等を考慮した追跡履歴の利用方法 ・知覚プロセスが物体の分類をへこうした場合、その物体の追跡履歴を考慮しなかった(1.5.5.2)	・追跡履歴の利用プロセスの決定／履歴がない場合のプロセスは安全全方向に定義されていたのか？	追跡履歴の利用プロセスは新規対象による新規予測が前提とするシステムであった （履歴を利用しない仕様であった）
A24	Software	予測プロセス　プレディクション（予測機能）	歩行者の移動方向が推定できること （歩行者はどの方向に動いているのか？）	・歩行者の移動方向を正しく認識しなかった ・対象物の切り替え等を考慮した追跡履歴の利用方法	A1-2. システムの設計には信号無視の歩行者への配慮が含まれていませんでした。(1.5.6.1)	ーーー 歩行者の分類について正確に知覚プロセスに渡すことについては報告書に記載がないため振り下げられないことより、ここまでとした。
A26	Software	予測プロセス　プレディクション（予測機能）	検出済みの物体については、追跡履歴を利用すること	・歩行者を正しく歩行者として分類されなかった ・信号無視の歩行者を歩行者として認識しなかった ・歩行者は横断歩道のない場所を横断していた	特定のオブジェクトの分類（「その他」）にはゴールが割り当てられていませんでした。現在検出されている位置は静的なものとみなされ、その位置が試験車両の道路上に直接ある場合を除き、その物体は障害物とはみなされませんでした。(1.5.5.2)	追跡履歴の利用プロセスは新規対象による新規予測が前提とするシステムであった （履歴を利用しない仕様であった）
A27	Software	予測プロセス　プレディクション（予測機能）	検出済みの物体について、移動体として認識されること	・歩行者を正しく歩行者として分類されなかった ・信号無視の歩行者を歩行者として認識しなかった ・歩行者は横断歩道のない場所を横断していた	特定のオブジェクトの分類（「その他」）にはゴールが割り当てられていませんでした。(1.5.5.2)	現在検出されている位置は静的なものとみなされ、その位置が試験車両の道路上に直接ある場合を除き、その物体は障害物とはみなされませんでした。
B1	Software	予測プロセス　プレディクション（予測機能）	歩行者の経路を正しく予測する。(1.5.6.1)	それまでの移動履歴を考慮していない(1.5.5.2)	システムの設計は、持続しない物体(分類が変更された物体)についての追跡履歴を除外したので、歩行者の経路を正しく予測することができなかった。(1.5.6.1)	衝突が発生したため、ATGは、システムがセンサー情報を融合し、可能性のある軌道を予測する方法を変更し、検出された物体が再分類されても追跡履歴を保持するようにしました(セクション1.9を参照)。(1.5.5.2)
B2	Software	コントロール	・自動での緊急制動の実施 ・オペレータによる緊急制動の実施	状況が衝突回避のための ADS の応答設計仕様（衝突を回避するためには 0.71g 以上の減速が必要）を超えていたため、緊急制動が抑制された(2.2.1.1)	・危険な状況を検知した後、衝突を防ぐために0.71g以上の急制動が必要な場合には、1秒間制動を抑制するようにADSを設計していました(2.2.1.1)	(1)システムが検出したハザードの性質を確認して代替経路を計算するか、(2)車両の運転者が衝突を制御する間、ADS が制動を抑制する 1 秒間であった。(1.5.5.3)
B3	Software	コントロール	・自動でのハンドル操作による回避 ・オペレータによるハンドル操作による回避	実際の係合解除時(1.5.4.2) ・行動抑制が始まる。(-1.2)	-1.2) ・自転車の周りを操縦するためのADSモーションプラン(0.3秒前に生成)ができなくなり、状況が危険(緊急事態)になる。 歩行者との衝突が迫っていると判断し、緊急事態を検知しました。 ・行動抑制が始まる。	車両内部の人間オペレータは、システムの操作を監視し、運転環境を監視し、必要に応じて車両の制御を取り、緊急時に介入することに任務を負った。(1.5.1)
B4	Software	コントロール	ADS開始後→オペレータへの車両制御の迅速な引き継ぎを確保を確保する必要がある。(1.4.5.3 オペレータプロトコル)	HMIと相互作用することによって、環境またはADS機能における異常事象を検出し、報告するように、車両オペレータに要求した(1.5.7.3D項に記載)。 (1.4.5.3 オペレータプロトコル)	オペレータの手と足が載せられていない状態の配慮不足。(1.8.3 オペレータ訓練)	具体的には、ハンドルの上に手を乗せて座り、ブレーキペダルの上に足を乗せる操作者は、注意を促し、必要に応じて操作者が迅速に制御できるように 設計された。(1.8.3 オペレータ訓練)
B6	Software	コントロール	衝突の恐れがある場合、車両を減速もしくは停止させる	減速はしたが、車両は停車させていなかった。	ATGは、誤報（危険な状況が存在しないのにADSが危険な状況を認識してしまうことで、車両が不必要に過激な操作を行う原因となる）を懸念して、行動抑制を実施した 緊急時の主な対応策は、危険を認識し、車両を制御し、適切に介入することが期待されている車両の運転手だった	最大制動速度 7m/s2、最大減速度 5m/s3 で衝突を回避できた場合には、システムは計画を実行し、最大許容値まで制動を行った。最大許容制動で衝突を回避できなかった場合には、車両の運転者に音声で警告すると同時に、車両の徐行を開始するように設計されていた
B8	Software	コントロール	システムが検出するべきであった	代替経路を計算しなかった	(1)システムが検出したハザードの性質を確認して代替経路を計算するか、(2)車両の運転者が車両を制御する間、ADS が制動を抑制する 1 秒間であった。(1.5.5.3)	ATG ADS操作中にボルボADASを解放したので、ボルボADASは、衝突時にアクティブではなかった
B9	Software	コントロール	緊急ブレーキが必要となった際、車両運転者に通知し、急ブレーキをかける。(1.5.6.1)	緊急ブレーキが必要な時に運転手に警報を鳴らしていない	衝突の19分25秒前に、システムは、ADSが係合解除中であることをオペレータに警告したことを示す。 (1.5.7 ヒューマンマシンインターフェイス)	HMIデータは、クラッシュの直前に、HMIがいかなる警報も提示しておらず、タグが入力されておらず、オペレータがクラッシュの前にHMIと対話していなかったことを示している。(2.2.2.1)
B10	Software	コントロール	システムは、緊急ブレーキをかけず、代わりに、車両を徐々に減速させる 計画を開始したときに、車両運転者に聴覚警報を鳴らした。(1.5.6.1)	緊急ブレーキが必要となった際、車両運転者に聴覚警報は鳴っていない。(1.5.6.1)	システムは、徐々に車両の減速を同時に開始しながら、車両運転者に聴覚的警告を送るように設計された。(1.5.5.3)	1.5.5.3 危険回避と緊急ブレーキ ADSが物体を検出し、分類し、追跡したとき、ADSは、急激な動きの変化なしに滑らかな動きを維持するために、車両のダイナミクス(操舵およびスロットル)を調節した。
B12	Software	ADS制御	係合解除時に、オペレータに聴覚警告を送る。(1.5.4.2)	ドライバーが係合解除の情報を無視し、ADSを再設定した。(1.5.7)	(-1.2) ・自転車の周りを操縦するためのADSモーションプラン(0.3秒前に生成)ができなくなり、状況が危険(緊急事態)になる。 歩行者との衝突が迫っていると判断し、緊急事態を検知しました。 ・行動抑制が始まる。 HMI はタブレット上でオペレータの入力を必要とする情報を一切表示しなかった。(1.5.7)	車両内部の人間オペレータは、システムの操作を監視し、運転環境を監視し、必要に応じて車両の制御を取り、緊急時に介入することに任務を負った。(1.5.1)
B13	Software	ADS制御	アクション抑制時にはアクション抑制が開始されたことを知らせる。(1.5.5.3)	アクション抑制が開始されたとき、オペレータに警告はなられなかった。(1.5.5.3)	緊急事態におけるまなお対策は、危険を認識し、車両を制御し、適切に介入することが期待された車両運転者であった。34(1.5.5.3) 34 車両運転者は、システムエラーまたは物体の誤分類に関連するのではなく、状況が真に衝突が切迫している場合にのみ入すことが期待された。	誤報（危険な状況が存在しないのにADSが危険な状況を認識してしまうことで、車両が不必要に過激な操作を行う原因となる）を懸念した(1.5.5.3)
B15	System	ADS制御	・前方衝突が迫っていることをドライバーに警告する(FCW) ・前方衝突を防止または軽減するために自動的にブレーキを開始する(AEB) (1.6)	ADASが動作しなかった	A1-1. ATGがATG ADSの運転中にボルボのADASを解除した(1.6.1)	SUVが自律モード(ATG ADSによって制御される)で動作されたとき、すべてのVolvo ADASコンポーネントは自動的に非アクティブ化された。 ・ボルボとATGシステムのレーダーは同じ周波数で作動するため、信号が誤解釈される可能性が高い ・SUVのブレーキモジュールは、ボルボAEBとATG ADSの両方からブレーキコマンドを受信する場合に優先順位を割り当てるように設計されていなかったため、互換性がないと考えられていた。
A11	Software	予測プロセスに移動する	歩行者の経路を正しく予測する。(1.5.6.1)	・歩行者の走行経路が正しく予測されなかった。	・走行車線で検出され、車両として分類された物体には、一般的にその車線の交通方向への走行目標が割り当てられる。(1.5.5.2) 前たに再分類された物体については、予測された経路はその目的に依存していた。(1.5.5.2)	ーーー 意思決定された状況や背景に関する記述はない
C1	Stakeholder	歩行者	歩行者進入禁止の車道に歩行者を侵入させない	歩行者が、自転車を押して歩行者横断禁止道路に侵入した。	歩行者が車道に物理的に入れないようにはなっていない。	車道全部にフェンス等を設けるのは不可能？ 歩きづらくすれば入ってこないと思った？
C2	Stakeholder	歩行者	歩行者進入禁止の車道に歩行者を侵入させない	歩行者が、自転車を押して歩行者横断禁止道路に侵入した。	歩行者が横断禁止の標識を認識できる状況・状態にない	意物反応あり
C3	Society	歩行者	歩行者進入禁止の車道に歩行者を侵入させない	歩行者が、自転車を押して歩行者横断禁止道路に侵入した。	歩行者が横断禁止の標識を認識できる状況・状態にない	午後9時58分頃であり、写真画像で確認する限り、街灯もほとんどなく、横断禁止の標識が見えていない。
C4	Society	歩行者	歩行者進入禁止の車道に歩行者を侵入させない	歩行者が、自転車を押して歩行者横断禁止道路に侵入した。	歩行者が車道に物理的に入れないようにはなっていない。	車道全部にフェンス等を設けるのは不可能？ 歩きづらくすれば入ってこないと思った？
C5	Society	歩行者	歩行者進入禁止の車道に歩行者を侵入させない	歩行者が、自転車を押して歩行者横断禁止道路に侵入した。	歩行者が車道に物理的に入れないようにはなっていない。 歩行者が横断禁止の標識を認識できる状況・状態にない	・車道全部にフェンス等を設けるのは不可能？歩きづらくすれば入ってこないと思った？ ・意物反応あり ・午後9時58分頃であり、写真画像で確認する限り、街灯もほとんどなく、横断禁止の標識が見えていない。
C6	Stakeholder	歩行者	法律を守る	アリゾナ州が歩行者に法律を守れるようにしていない	・夜でも横断禁止の標識が見えるようにはなっていない。 ・正常な判断ができる状態にかった	・車道全部にフェンス等を設けるのは不可能？歩きづらくすれば入ってこないと思った？ ・意物反応あり ・午後9時58分頃であり、写真画像で確認する限り、街灯もほとんどなく、横断禁止の標識が見えていない。
C7	Society Service	歩行者	安全・安心な環境の提供	NHTSA（米国道路交通安全局）SAE（旧自動車技術者協会）ATG（先端技術グループ(Uber)）がドライバーに警告する仕組みを準備しない	・異常者の行動を前提にしていない ・歩行者が標識を見てする前提となっている ・歩行者が車道に入ってこない前提となっている ・ドライバーが正しく運転する前提になっている	？
C8	Stakeholder	ATG	・安全文化・方針を定める ・安全管理が行われていることを確認する ・安全管理が責任を果たし、リスクと損失防止評価、安全管理の履行を行っていることを確認する	・ADSを公道でテストするリスクを評価しない ・安全管理者の業務が行われていることを確認をしない	・安全管理者の代表的な業務（安全説明会の実施、運転上のリスクと損失防止の評価、安全文化の維持）を組織として行っていない ・企業としての安全文化・方針の浸透状況を確認していない	1.8.2 ・安全の説明、運転上のリスクと損失防止評価、安全文化の維持を担う責任の組織がなく、作業員が安全管理者の任務を負っている ・（安全管理者の業務が行われているとの）スポット確認の頻度の記録がない
C9	Stakeholder	ATG	ドライバーに対してUberの安全文化・方針を認識させる	ドライバーに対して、携帯電話の使用に特化した方針に署名をさせ、受領させていない	安全に関する方針があり教育を行っているが、携帯電話を使用しないことを確実に遵守させるための手続きが行われていない	64(a) 従業員は、携帯電話の使用に特化した方針のコピーに署名したり、受け取ったりしなかった
C10	Stakeholder	ATG	Uberの安全文化・方針に従わないドライバーの違反を確実に検出する	① ・オペレータに対する車物検査を実施 ・ATGへの方針違反がオペレーターの自己報告、または同僚による報告 ・ターミナル・マネジャーがビデオを調べて遵守状況確認 ② 事故を起こしたドライバーの違反調査が行われていない	① 違反者の抽出・意味が確実に行われる基準が設定されていない ・車物検査を毎回行う ・方針違反の報告義務 ・ビデオ調査のタイミングと調査方法に対するリスク評価 ② ドライバーの違反調査の仕組み（実施と記録）の欠如	①1.8.2 ・車物検査の散発的な実施 ・方針違反の報告は禁助（義務ではない） ・ビデオ調査は無作為でスポット実施 ・スポットチェックは違反報告後のみ ①1.8.2 ・治験責任医師は、ATGが、Tempe衝突前に、衝突に関与した車両運転者のビデオ記録を調べたという証拠を見つけなかった。同僚からの報告はなく、就職中に懸戒処分を受けなかった。インタビューを受けたとき、彼女の上司はオペレータのビデオをレビューすることを報告しなかった。
C11	Stakeholder	ATG	自動車運転時にドライバーの違反を抽出するような監視を行う	・自動運転中にドライバーの任務遂行状況に関する監視が行われていない	自動運転時にドライバーの監視を行う仕組みが欠如	・衝突に関与した車両運転者のビデオ記録を調べていない ・上司はオペレータのビデオをレビューすることを報告していない ・単体オペレーターによる操作のため、同僚による報告はそもそも行われていない ・単一オペレータへの移行は、ATGが試験車両の数を増やすための運用上の決定
C12	Stakeholder	ATG	ドライバーにUberの安全文化・方針を遵守させる	ドライバーによる携帯電話の使用に特化した方針の署名を行っていない	安全に関する方針があり教育を行っているが、違反に対する従業員に携帯電話を使用しないことなど、遵守させるための署名が行われていない	64(a)従業員は、携帯電話の使用に特化した方針のコピーに署名したり、受け取ったりしなかった
C13	Society	ADOT	ADS試験を実施する事業体へ自動運転車である書面を提出させる	ADOTの自動車両試験の監督が当該開発者に対して行われなかった	ADOTに対し、自動車であることを確認する書面を提出する必要があるのは、無人ADS搭載車を試験する開発者(車内に人がいない場合)のみであった	
C14	Stakeholder	NHTSA	連邦レベルで ・自動運転車に対する安全基準を策定する ・安全上の欠陥が発見された場合に規格を実施し、行動する権限を有する	・1.10.1 ・自動運転車を発表 2016.9 ADS開発者に安全性自己評価報告書を機関に提出するよう求めるプロセスの計画を概説 2017.9 ・12の安全要素を記載。安全自己評価報告書の作成に使用するために製造業者などに要約ガイダンスを提供 ・開発者は各要素の目標を達成するためのプロセスを作成することを奨励 本報告書の目付現在、 ・FCW,AEB,ADSなどのシステムに必要な安全基準の策定なし、 ・最小ADS性能を評価するための試験手順の提案なし	開発者がどのようにこれらの目標を達成すべきかの具体的な情報はほとんど得られなかった。また、開発者やほかの人々に、自分たちの安全プロセスを評価する手段を提供しなかった この方針は、自動車の開発時に開発者がガイダンスを遵守すること、または安全自己評価報告書を提出することを要求しなかった。この方針は、評価報告書が提出された場合、NHTSAの承認を受けなかった	・2016年9月に、自動車に関する初期方針文書を公表（ADS搭載車両の試験及び配備に関する基本的な指針を示した）。また、車両内部にオペレータを持つための要件によって作成された自律的な車両使用に対する規制物の除去に焦点をあてたモデル性能方針を提案 ・第10 政策：ADS開発者に安全性自己評価報告書を機関に提出するよう求めるプロセスの計画を概説。（自主的、将来的に義務付けられるかもしれない） ・第2次自動車政策2017.9 12の安全要素を記載。安全自己評価報告書の作成に使用するために製造業者などに要約ガイダンスを提供 開発者は各要素の目標を達成するためのプロセスを作成することを奨励
C15	Stakeholder	AAMVA	アリゾナ州に対して自動運転車の安全に対する対策に関与する	アリゾナ州に対して自動運転車の安全対策に関与していない		AAMVAは管理、法執行、モデルプログラム開発を開発。高速道路の安全問題のための情報交換所としての役割を果たす。国及び地方自治体の職員を代表する団体
C16	Society	FMVSSs	自動運転システムに対しても安全基準や評価（審査）の仕組みを提供する	自動運転システムに関する安全基準や評価の仕組みを提供しない	ADSの運転安全基準及び評価プロトコルが欠如	NTSBの報告では、国家レベルでのADSの運用安全基準と評価プロセスについて動向の記載なし
C17	Stakeholder Service	ドライバー	ドライバーは運転中、車道から目を離さず、携帯電話もみない	ドライバーが運転中に車道から目を離し携帯電話を使用した	自動運転車両でのドライバーの責務を全うしていない	
C18	Stakeholder Service	ドライバー	ドライバーが携帯電話使用等のポリシーに対して署名する	ドライバーが運転中に携帯電話を使用した	署名していない	-

改善前のCS図


Society
連邦自動車安全基準
(FMVSSs)
規格
<process model>
* ISO 26262
* SOTIF
* Cybersecurity
アリゾナ州法律
(歩行者の責任)
アリゾナ州法律
(ドライバーの責任)
Stakeholder
高速道路交通安全局
(NHTSA)
参照
参照
参照
反応
アリゾナ州
<process model>
* 行政命令
- 2015-09
- 2018-04
行政命令
アリゾナ州運輸省
Uber Advanced
Technologies Group
対策
部品供給者
- 薬物反応あり
- 法律違反して道路を横断
歩行者
Service
検知
検知
検知
検知
前方道路を見ていなかった。（前方不注意）
携帯電話でテレビで番組を見ながら業務。（業務態度）
ドライバー
ADS設定(ON -> OFF)
（衝突の19分12秒前）
操作（衝突の0.7s後）
操作（衝突の0.02s前）
System
警報
（衝突の19分25秒前）
（操作されていない状態）
スピーカー
HMI
ブレーキペダル
アクセルペダル
ハンドル
自動運転
OFF -> ON
操作量
操作量
操作量
ライダー
レーダー
カメラ
GPS
ブレーキシステム
エンジン
ステアリングシステム
ライダーデータ
レーダーデータ
画像データ
位置情報
ブレーキ操作
（衝突の0.7s後）
アクセル量
ステアリング量
⇒ADS解除
（衝突の0.2s前）
アクセル操作
自動運転ON/OFF
ブレーキ操作
（衝突の0.7s後）
ステアリング量
⇒ADS解除
（衝突の0.2s前）
ADAS
Software
ADS
警報ON
ブレーキ量
アクセル量
ステアリング量
知覚プロセス
パーセプション（認識技術）
ADS制御（ADSのON/OFF）
コントロール
自転車を押している歩行者を歩行者と認識しなかった
-3.8~2.7：分類が車両と他で数回交代。ADSはオブジェクトの経路を静的として予測。
認識データ
想定進路
プレディクション（予測機能）

改善後のCS図


Society
連邦自動車安全基準
(FMVSSs)
自動運転に関する
連邦自動車安全基準
規格
<process model>
* ISO 26262
* SOTIF
* Cybersecurity
アリゾナ州法律
(歩行者の責任)
アリゾナ州法律
(ドライバーの責任)
制定
制定
Stakeholder
高速道路交通安全局
(NHTSA)
自動車管理者協会
法整備等に関与
参照
反応
自動運転に関する基準・
評価の仕組みを整備
制定
制定
Uber Advanced
Technologies Group
対策
部品供給者
参照
参照
アリゾナ州
<process model>
* 行政命令
- 2015-09
- 2018-04
行政命令
アリゾナ州運輸省
統制
企業の安全管理
安全リスクマネジメント
自転車のメンテナンス
交通ルールを徹底する教育
歩行者
自動運転に関する法律等の整備
・運転者を内部に置いた自動運転車試験に関する要求
・自動運転時の運転者の状態を管理、監視する機能の義務化などの法整備
・自動運転時の運転手の不注意に関する法整備
・自動運転自動車対歩行者の法律上の定義
・自転車のメンテナンス
乗車態度の監視
重要事項確認（雇用開始時、定期的）
報告
Service
ドライバー
検知
検知
検知
検知
検知
ADSを解除した際に解除した理由をドライバーに通知する仕組み
操作
操作
System
外部からの入力
警報
ADS解除理由
ADS設定
(ON <-> OFF)
ADS設定可否
スピーカー
HMI
ブレーキペダル
アクセルペダル
ハンドル
操作量
操作量
操作量
熱源感知
センサー
音声感知
センサー
ライダー
レーダー
カメラ
GPS
ADS解除理由
自動運転
OFF <-> ON
ブレーキシステム
エンジン
ステアリングシステム
熱情報
音声情報
ライダーデータ
レーダーデータ
画像データ
位置情報
ブレーキ量
ブレーキ量
ステアリング量
アクセル量
アクセル量
ステアリング量
画像データ
ADAS
アクセル量
ステアリング量
ブレーキ量
ブレーキ量
アクセル量
ステアリング量
制度向上
Software
ADS
物体検出用に搭載するカメラ、センサーのスペックについて十分な検証を行い、基準を制定する必要がある
警報ON
ブレーキ量
（急制動含む）
アクセル量
（急制動含む）
ステアリング量
（急制動含む）
知覚プロセス
パーセプション（認識技術）
ADS制御（ADSのON/OFF）
停止制御
（ADS突然解除時）
コントロール
対象物について「交通ルールが遵守されない」ことに対するリスク検討・安全性向上に向けた冗長的なロジック検討し追加することで事故を回避できる可能性がある。
対象物について「交通ルールが遵守されない」ことに対するリスク検討・安全性向上に向けた冗長的なロジック検討し追加することで事故を回避できる可能性がある
「警報無視」、「警報切」による運転手の不安全行動への対応として、自動で車両停止等による安全性確保に向けた冗長的な仕組みを検討
安全方向に対応するのであれば、自動運転にて停止を最優先する
対象物について「交通ルールが遵守されない」ことに対するリスク検討・安全性向上に向けた冗長的なロジック検討し追加することで事故を回避できる可能性がある
認識データ
「知覚に関するコンポーネント」⇔「予測に関するコンポーネント」の機能連携等の機能拡充
想定進路
機能連携等の機能拡充
プレディクション（予測機能）
対象物について「交通ルールが遵守されない」ことに対するリスク検討・安全性向上に向けた冗長的なロジック検討し追加することで事故を回避できる可能性がある。

付録6_表3：抽象的コンポーネントレベルでの分析結果

No	カテゴリ5階層をイメージ	高位レベルの事象（抽象的事象）	CAST6-1	CAST6-2	CAST6-3	CAST6-4
			安全上の責務(責任)	非安全なコントロールアクション (CSI図の赤矢印をイメージ)	プロセス/メンタルモデルの欠陥	意思決定された状況・背景
A2	System	カメラ、センサ	・捉えた映像を正確に知覚プロセスに渡すこと。	ーーー カメラの映像について正確に知覚プロセスに渡すことについては報告書に記載がないため振り下げられないことより、ここまでとした。	ーーー	ーーー
A5	Software	知覚プロセス パーセプション（認識技術）	対象物を正しく分類する カメラ、ライダー、レーダーの情報から対象物を正しく識別する	(1-1)・対象（歩行者）を正しく判断できない条件があった	(1-1)・信号無視の歩行者を歩行者として認識する設計になっていなかった。 (1-2)・横断歩道付近以外の歩行者についても、明示的なゴールを設定しない設計であった。(1.5.5.2)	(1-1)・アリゾナ州の法律では、歩行者は車道を渡ってはならないとなっている。 (1-2)・アリゾナ州の法律では、車道を横断する歩行者は走行する全ての車両に道を譲らなければならない法律になっていた（1.7.4）
A11					(1-3) 走行車線で検出され、車両として分類された物体には、一般的にその車線の交通方向への走行目標が割り当てられる。(1.5.5.2)	
A12				(2-1)ADSは、対象（歩行者）の分類を他の対象（車両、自転車、その他）と交互に数回変更たが正しく部類されなかった。(1.5.6.1)	持続しない物体(分類が変更された物体)についての追跡履歴を除外したので、歩行者の経路を正しく予測することができなかった。(1.5.6.1)	
A13	System	カメラ、センサ	・捉えた映像を正確に知覚プロセスに渡すこと。（運転手が見ている状況と同じ情報が取得できること）	夜間の状況、並びに解像度及びカメラレンズの品質に依存した状況であった。(1.5.6.2) (1-1)運転手が見ているものを正確に描写できなかった	ーーー	・新しく販売された自転車は、前部、後部、およびペダルに反射器を有し、車輪の側壁またはスポークに側面反射器を有することを要求されていた。 ・車輪スポークに側面反射器を有したものを自転車と設計していた？ ・自転車のライトが地面に垂直に照らさせていたから自転車として認識しなかった？
A17	Software	予測プロセス　プレディクション（予測機能）	対象（歩行者）の移動方向を正しく認識する	(1-1)対象（歩行者）の移動方向を正しく認識しなかった (2-1)物体の分類を変更した場合、その物体の追跡履歴を考慮しなかった	(1-1)(2-1)物体の分類が変更された場合、それまでの履歴を利用しない仕様だった。	ーーー
A24-1	Software	予測プロセス　プレディクション（予測機能）	対象（歩行者）の移動速度を正しく認識できる 追跡履歴に基づいて、可能性のある軌跡（進路予測）を生成する(1.5.5.2) 進路を継続的に更新する(1.5.5.2)	(1-1)・対象（歩行者）の移動方向を正しく認識しなかった	(1-1) システムの設計には信号無視の歩行者への配慮が含まれない(1.5.6.1)	ーーー 歩行者の分類について正確に知覚プロセスに渡すことについては報告書に記載がないため振り下げられないことより、ここまでとした。
A24-2				(1-1)・対象物の切り替え等を考慮した追跡履歴の利用方法 (1-2)・知覚プロセスが物体の分類を変更した場合、その物体の追跡履歴を考慮しなかった(1.5.5.2)	(1-1)・信号無視の歩行者を歩行者として認識する設計になっていなかった。 (1-2)・横断歩道付近以外の歩行者についても、明示的なゴールを設定しない設計であった。(1.5.5.2)	(1-1)・アリゾナ州の法律では、歩行者は車道を渡ってはならないとなっている。 (1-2)・アリゾナ州の法律では、車道を横断する歩行者は走行する全ての車両に道を譲らなければならない法律になっていた（1.7.4）
A26	Software	予測プロセス　プレディクション（予測機能）	検出済みの物体については、追跡履歴を利用する	(1-1)・信号無視の歩行者を歩行者として認識しなかった (1-2)・歩行者は横断歩道のない場所を横断していた	(1-1)・信号無視の歩行者を歩行者として認識する設計になっていなかった。 (1-2)特定のオブジェクトの分類（「その他」）にはゴールが割り当てられていなかった。 現在検出されている位置は静的なものとみなされ、その位置が試験車両の進路上に直接ある場合を除き、その物体は障害物とはみなされませんでした。(1.5.5.2)	(1-1)履歴を利用しない仕様であった
A27	Software	予測プロセス　プレディクション（予測機能）	検出済みの物体について、移動体として認識される	(1-1)・歩行者を正しく歩行者として分類されなかった (1-2)・信号無視の歩行者を歩行者として認識しなかった ・歩行者は横断歩道のない場所を横断していた	同上	(1-1)現在検出されている位置は静的なものとみなされ、その位置が試験車両の進路上に直接ある場合を除き、その物体は障害物とはみなされませんでした。
B1	Software	予測プロセス　プレディクション（予測機能）	歩行者の経路を正しく予測する。(1.5.6.1)	(1-1)それまでの移動履歴を考慮していなかった(1.5.5.2)	(1-1)システムの設計は、持続しない物体(分類が変更された物体)についての追跡履歴を除外したので、歩行者の経路を正しく予測することができなかった。(1.5.6.1)	(1-1)衝突が発生したため、ATGは、システムがセンサー情報を融合し、可能性のある軌道を予測する方法を変更し、検出された物体が再分類されても追跡履歴を保持するようにしました(セクション1.9を参照)。(1.5.5.2)
B2-1	Software	コントロール	・自動での緊急制動の実施	(1-1)状況が衝突回避のための ADS の応答設計仕様（衝突を回避するためには 0.71g 以上の減速が必要）を超えていたため、緊急制動が抑制された(2.2.1.1)	(1-1)・危険な状況を検知した後、衝突を防ぐために0.71g以上の急制動が必要な場合には、1秒間制動を抑制するようにADSを設計していた(2.2.1.1)	(1-1)システムが検出したハザードの性質を確認して代替経路を計算する (1-2)車両の運転者が車両を制御する間、ADS が制動を抑制する 1 秒間であった。(1.5.5.3)
B2-2	Software	コントロール	・オペレータによる緊急制動の実施	(1-1)オペレーターが長時間車道から離れて視界を見ていた 電話上のアプリケーションを使用してテレビ番組を見ていた。(1.1)	(1-1)緊急事態における主な対策は、危険を認識し、車両を制御し、適切に介入することが期待された車両運転者であった。(1.5.5.3)	(1-1)ADSが歩行者との衝突が切迫していると判断したとき、システムの設計とATGの軽減戦略は、車両の制御を車両運転者に頼っていた(2.2.2)
B3-1	Software	コントロール	・自動でのハンドル操作による回避	突然の係合解除時(1.5.4.2) ・行動抑制が始まる。(-1.2)	(-1.2) ・自転車の周りを操縦するためのADSモーションプラン(0.3秒前に生成)ができなくなり、状況が危険(緊急事態)になる。 歩行者との衝突が迫っていると判断し、緊急事態を検知しました。 ・行動抑制が始まる。	(1-1)車両内部の人間オペレータは、システムの操作を監視し、運転環境を監視し、必要に応じて車両の制御を取り、緊急時に介入することに任務を負った。(1.5.1)
B3-2	Software	コントロール	・オペレータによるハンドル操作による回避	(1-1)オペレーターが長時間車道から離れて視界を見ていた 電話上のアプリケーションを使用してテレビ番組を見ていた。(1.1)	(1-1)緊急事態における主な対策は、危険を認識し、車両を制御し、適切に介入することが期待された車両運転者であった。(1.5.5.3)	(1-1)ADSが歩行者との衝突が切迫していると判断したとき、システムの設計とATGの軽減戦略は、車両の制御を車両運転者に頼っていた(2.2.2)
B4	Software	コントロール	車両制御（自動化、手動化）の迅速な引き継ぎの実施(1.4.5.3 オペレータプロトコル)	車両制御の異常検出時に、運転者の操作が必要(1.5.7.30項に記載)。(1.4.5.3 オペレータプロトコル)	異常検出時に運転者への警告I/Fへの配慮不足(1.8.3 オペレータ訓練)	運転者は、ハンドルの上に手を乗せて座り、ブレーキペダルの上に足を乗せる前提の設計(1.8.3 オペレータ訓練)
B6	Software	コントロール	衝突の恐れがある場合、車両を減速もしくは停止させる	行動抑制の実施に伴い十分に減速できない、もしくは停車できない	・システムの誤報を懸念して、行動抑制を実施する設計。 ・緊急時の対応は車両の運転者だった。	最大許容制動で衝突を回避できない場合は、車両の運転者に音声で警告し、車両の操作を開始する設計。
B8	Software	コントロール	対象物を正しく分類する	代替経路を計算しなかった	運転者が車両を制御する間、ADS が制動を抑制（１秒間）する設計(1.5.5.3)	安全の冗長性がない設計であった。
B9	Software	コントロール	緊急ブレーキが必要時に聴覚警報を鳴らす。(1.5.6.1)	急ブレーキが必要な時に運転手に警報を鳴らしていない	システムは事前にADSが係合解除中であることを運転者に警告したが、運転者に無視された。 (1.5.7 ヒューマンマシンインターフェイス)	運転者と車両間でのI/Fに配慮不足があった。(2.2.2.1)
B10	Software	コントロール	車両を減速させる際、運転者に聴覚警報を鳴らす。(1.5.6.1)	緊急ブレーキの必要時、聴覚警報が鳴っていない。(1.5.6.1)	徐々に減速を開始しながら、運転者に聴覚的警告を送る設計(1.5.5.3)	自動による危険回避、緊急ブレーキ時、急激な動きの変化なしに滑らかな動きを維持するよう、車両抑制する設計（1.5.5.3）
B12	System	ADS制御	係合解除時に、運転者に聴覚警告を送る。(1.5.4.2)	ドライバーが係合解除の情報を無視し、ADSを再設定した。(1.5.7)	HMI はタブレット上でオペレータの入力を必要とする情報を一切表示しなかった。(1.5.7)	運転者は、システムの挙動、運転環境を監視し、緊急時に介入することに任務を負う。(1.5.1)
B13	System	ADS制御	車両抑制時には抑制が開始を知らせる。(1.5.5.3)	車両抑制時、運転者に警告がなかった。(1.5.5.3)	緊急時に運転者が車両を制御する設計(1.5.5.3)	誤報の懸念を考慮した(1.5.5.3)
B15	System	ADS制御	(1.6) ・ 前方衝突が迫っていることをドライバーに警告する (FCW) ・ 前方衝突を防止または軽減するために自動的にブレーキを開始する (AEB)	(1-1)ADASを無効にしていた	(1-1)レーダーの誤動作に関する検証ができていない (1-2)ブレーキコマンド受信時の優先順位が設計されていない (1-3)ADASを併用しようとした場合、開発に時間がかかると考えられていた？	(1-1)ボルボとATGシステムのレーダーが同じ周波数で作動するため、誤動作すると考えていた (1-2)ボルボAEBとATG ADSの両方からブレーキコマンドを受信した場合、正しく動作しないと考えていた。
A11	Software	予測プロセス　プレディクション（予測機能）	歩行者の経路を正しく予測する。(1.5.6.1)	(1-1)歩行者の走行経路が正しく予測されなかった。	(1-1)新たに再分類された物体の予測た経路はその目的に依存していた。(1.5.5.2)	ーーー 意思決定された状況や背景に関する記述はない
C1 C2	Stakeholder	歩行者	法律を守らせる	アリゾナ州が歩行者に法律を守れるようにしていない	歩行者が標識を見て守る前提となっている	人は法律を守る
C3	Society	歩行者	法律を守らせる	アリゾナ州が歩行者に法律を守れるようにしていない	歩行者が標識を見て守る前提となっている	人は法律を守る
C4 C5	Society	歩行者	法律を守らせる	アリゾナ州が歩行者に法律を守れるようにしていない	歩行者が車道に入ってこない前提となっている	車道全部にフェンス等を設けるのは不可能？ 歩きづらくすれば入ってこないと思った？
C6	Stakeholder	歩行者	法律を守る	歩行者が法律に違反する	異常者の行動を前提にしていない	
C7	Society Service	歩行者	安全・安心な環境の提供	NHTSA（米高速道路交通安全局）SAE（旧自動車技術者協会）ATG（先端技術グループ(Uber)）がドライバーに警告する仕組みを準備しない	・異常者の行動を前提にしていない ・歩行者が標識を見て守る前提となっている ・歩行者が車道に入ってこない前提となっている ・ドライバーが正しく運転する前提になっている	?
C8	Stakeholder	ATG	・安全文化・方針を定める ・安全管理が行われていることを確認する ・安全リスクマネジメントの実施	企業としての安全管理の業務を組織として行っていない 安全リスクマネジメントが行われていない	安全管理体制が甘い 企業の安全文化・方針浸透を確認しない	
C9	Stakeholder	ATG	安全方針の遵守と徹底	従業員が遵守すべき個別重要事項の確認行為を行っていない	個別遵守確認の欠如	
C10	Stakeholder	ATG	安全方針の遵守と徹底	従業員の遵守状況の検査が行われていない	安全保証の基準の設定なし	
C11	Stakeholder	ATG	車両運転者監視 業務実行時の監視とコントロール	従業員の車両運転時の監視を行っていない	運転者の異常検知とフィードバックが不十分	
C12	Stakeholder	ATG	安全方針の遵守と徹底	従業員が遵守すべき個別重要事項の確認行為を行っていない	個別遵守確認の欠如	
C13	Society	ADOT	州としての企業に対する安全監督・統制	自動運転の試験を行う企業に対する統制行為の対象が（リスクに対応して）網羅されていない	当該事項に対するリスク分析と対策が不十分	
C14	Stakeholder	NHTSA	連邦レベルで ・自動運転車に対する安全基準を策定する ・安全上の欠陥が発見された場合に規格を実施し、行動する権限を有する	自動運転車に関する 安全性自己評価プロセスが不十分 ・安全基準の策定 ・性能評価の試験手順の提示 が具体的でない	方針は示しているものの、対象者が具体的に対処できるような行動指針・遵守レベルが不明瞭かつ示されていない	
C15	Stakeholder	AAMVA	安全対策の開発者（AAMVA）が、連邦のすべての州に対して(新技術を含む）自動車の安全対策の統制に関与する	AAMVAが連邦のすべての州と事業者に対して新技術含む安全対策に対する統制に関与していない	新技術を含む安全対策へのアプローチがプロセスかされていない？(各州間の連携含め)	
C16	Society	FMVSSs	新技術のシステムに関して、国家レベルでの安全基準や評価の仕組みを設定する(見直される)	新技術のシステムに対する安全基準や評価の仕組みがない	新技術のシステムに対する安全基準や評価をどう取り扱うかのプロセスがない？	（国家レベルでの安全基準や評価プロセスについての記載なし）
C17	Stakeholder Service	ドライバー	ドライバーが状況にあわせて車両コントロールする	ドライバーが状況を把握しようとしていない（安全義務を放棄している）	自動運転車両でのドライバーの責務を全うしていない	自動運転への過信
C18	Stakeholder Service	ドライバー	ドライバーは運転に集中する	運転に集中していない	自動運転車両とドライバーの責務が曖昧になっている。	自動運転への過信

付録7_表4：システムの俯瞰分析結果

●最頻的要因／○●から影響すると思われる要因

NO	欠陥	CAST手順	コンポーネント	欠陥分類	KeyWord1	KeyWord2	Society	Stakeholder	Service	System	Software	CAST7（対策）					CAST8（提示）
												安全リスク評価・冗長性	運転手への配慮	設計手順 ・考慮漏れ	ドライブセンサの能力	安全なマネジメントシステムの設計	安全な文化	時間的な変化とダイナミクス
A23-1	(1-1)運転手が言っているものを正確に理解できなかった	CAST6-2	カメラ、センサ	UCA	対象物の認識	検知できない	–	–	–	● カメラの解像度等	–				● カメラの解像度等			● カメラ映像の時間的な変化
A23-2	（新しく発売された自動車は、前面、後面、およびボディに反射器を有し、車輪の側面または車輪スポークに側面反射器を有することを要求されている。	CAST6-4	知覚プロセス パーセプション（認識技術）	車両決定状況・背景	対象物の認識	正しく分類できない	● 法律に依存				–					● 法律に依存		● 法律に依存
A23-3	「車輪スポークに側面反射器を有したもの」を自動車と認識していた？	CAST6-4	知覚プロセス パーセプション（認識技術）	車両決定状況・背景	対象物の認識	正しく分類できない	● 法律に依存	○ 法律に依存	–		○ 法律に依存					● 法律に依存		○ 法律に依存
A13-4	「自転車のライトが他車に幾度に幾度に幾度にすぐいたから自転車と認識しなかった？	CAST6-4	知覚プロセス パーセプション（認識技術）	車両決定状況・背景	対象物の認識	正しく分類できない	–	● 自転車用若者	–		–		○ 自転車用若者					● 自転車用若者
A17-1	(1-1)対象（歩行者）の移動方向を正しく認識しなかった	CAST6-2	予測プロセス プレディクション（予測機能）	UCA	対象物の制御	移動方向の分析誤り	–	○ 設計不備	–		● 設計不備	○ 設計不備		● 設計不備				
A17-2	(2-1)物体の分類を変更した場合、その物体の追跡履歴を考慮しなかった	CAST6-3	予測プロセス プレディクション（予測機能）	UCA	対象物の制御	移動方向の分析誤り	–	○ 設計不備	–		● 設計不備	○ 設計不備		● 設計不備				
A17-3	(1-1)(2-1)物体の分類が変更された場合、それまでの履歴を利用しない仕様だった。	CAST6-3	予測プロセス プレディクション（予測機能）	プロセス/メンタルモデル	対象物の制御	移動方向の分析誤り	–	○ 設計不備	–		● 設計不備	○ 設計不備		● 設計不備				
A11-1	(1-1)歩行者の走行経路がまくい予測されなかった。	CAST6-2	予測プロセス プレディクション（予測機能）	UCA	対象物の制御	移動方向の分析誤り	–	○ 設計不備	–		● 設計不備	○ 設計不備		● 設計不備				
A11-2	(1-1)前に車台間さんを物体の予測と経路はその前前に保存していた。(1.5.5.2)	CAST6-3	予測プロセス プレディクション（予測機能）	プロセス/メンタルモデル	対象物の制御	移動方向の分析誤り	–	○ 設計不備	–		● 設計不備	○ 設計不備		● 設計不備				
A12-1	(1-1)・対象（歩行者）の移動方向を正しく認識しなかった	CAST6-2	知覚プロセス パーセプション（認識技術）	UCA	対象物の認識	分類できない	● 法律に依存	○ 法律に依存	–	○ カメラ検出に依存	○ 法律に依存	○ 設計不備		○ 安全リスク評価・冗長性に依存	○ カメラ検出に依存	● 法律に依存	● 歩行者に依存	● 法律の形態化に依存
A12-2	(1-1)システムの設計には信号無視の歩行者への配慮が含まれない(1.5.6.1)	CAST6-3	知覚プロセス パーセプション（認識技術）	プロセス/メンタルモデル	対象物の認識	分類できない	● 法律に依存	○ 法律に依存	–	○ カメラ検出に依存	○ 法律に依存	○ 設計不備		○ 安全リスク評価・冗長性に依存	○ カメラ検出に依存	● 法律に依存	● 歩行者に依存	● 法律の形態化に依存
A24-2	(1-1)・対象物の切り替え等を考慮した自動運転の利用方法 (1-2)・知覚プロセスが物体の分類を変更した場合、その物体の追跡履歴を考慮しなかった(1.5.5.2)	CAST6-2	知覚プロセス パーセプション（認識技術）	UCA	対象物の追跡履歴	履歴を考慮しない	● 法律に依存	–	–	○ 設計に依存	○ 法律に依存	● 設計不備		○ 安全リスク評価・冗長性に依存	–	–	–	–
A26	(1-2)特定のオブジェクトの分類（「その他」）にはゴールが割り当てられていなかった。 物体検出されている位置は静的なものとみなされ、その位置が試験車両の進路上に直接ある場合を除き、その物体は障害物とはみなされませんでした。(1.5.5.2)	CAST6-3	知覚プロセス パーセプション（認識技術）	プロセス/メンタルモデル	信号無視	認識しない	● 法律に依存	○ 法律に依存	–	○ 法律に依存	○ 法律に依存	● 設計不備		○ 安全リスク評価・冗長性に依存	○ カメラ検出に依存	○ 法律に依存	● 歩行者に依存	● 法律の形態化に依存
A27	(1-1)物体検出されている位置は静的なものとみなされ、その位置が試験車両の進路上に直接ある場合を除き、その物体は障害物とはみなされませんでした。	CAST6-4	知覚プロセス パーセプション（認識技術）	車両決定状況・背景	対象物の認識	静的なもの	● 法律に依存	–	–	○ カメラ検出に依存	○ 法律に依存	● 設計不備		○ 安全リスク評価・冗長性に依存	○ カメラ検出に依存	● 法律に依存	● 歩行者に依存	● 法律の形態化に依存
B1	(1-1)衝突が発生したため、ATGは、システムがセンサー情報を融合し、可能性のある軌道を予測する方法を変更し、検出された物体が物理的に占める追跡履歴を保持するようにしましたが(セクション1.9を参照)。(1.5.5.2)	CAST6-4	知覚プロセス パーセプション（認識技術）	車両決定状況・背景	対象物の認識	停止物	● 法律に依存	–	–	○ カメラ検出に依存	○ 法律に依存	● 設計不備		○ 安全リスク評価・冗長性に依存	○ カメラ検出に依存	● 法律に依存	● 歩行者に依存	
B2-1-1	(1-1)状況が複雑回避のための ADS の応答設計仕様（衝突を回避するために 0.7は以上の減速が必要）を超えていたため、緊急制動が回避された(2.2.1.1)	CAST6-2	知覚プロセス パーセプション（認識技術）	UCA	対象物の認識	移動履歴	● 法律に依存 （周辺の車両への配慮）	–	–	○ カメラ検出に依存	● 法律に依存 （周辺の車両への配慮）	● 設計不備		○ 安全リスク評価・冗長性に依存	○ カメラ検出に依存	● 法律に依存	● 歩行者に依存	–
B2-1-2	(1-1)・危険な状況を検知した後、衝突を回避するために0.71g以上の急制動が必要な場合には、1秒間制動を回避するようにADSを設計していた(2.2.1.1)	CAST6-3	知覚プロセス パーセプション（認識技術）	プロセス/メンタルモデル	対象物の認識	回避履歴	● 法律に依存 （周辺の車両への配慮）	–	–	○ カメラ検出に依存	● 法律に依存 （周辺の車両への配慮）	● 設計不備		○ 安全リスク評価・冗長性に依存	○ カメラ検出に依存	● 法律に依存	● 歩行者に依存	–
B2-1-3	(1-1)システムが検出したカーボーカの挙動を確認して代替経路を計算する (1-2)車両の運転手が衝突を制御する間、ADS が制動を回避する 1 秒間であった。(1.5.5.3)	CAST6-4	知覚プロセス パーセプション（認識技術）	車両決定状況・背景	対象物の認識	停止物	–	–	–	○ カメラ検出に依存	● 設計不備	● 設計不備		○ 安全リスク評価・冗長性に依存	○ カメラ検出に依存	● 法律に依存	● 歩行者に依存	
B2-2-1	(1-1)オペレーターが長時間車速から離れて活用を主でいた 物体上のプリケーションを使用してテレビ電話を見ていた。(1.1)	CAST6-2	コントロール	UCA	オペレーター		● 法律に依存	●運転手に依存	–	○ カメラ検出に依存	–	○ 運転手への配慮に依存	● 運転手に依存	○ 運転手への配慮に依存	● 運転手に依存	○ 車内カメラ検出に依存	○ 法律に依存	○ 運転手に依存
B2-2-2	(1-1)緊急事態における走る対策は、危険を認識し、衝突を制御し、適切に介入することが期待された車両運転手であった。(1.5.5.3)	CAST6-3	コントロール	プロセス/メンタルモデル	オペレーター	運転手の位置づけ	● 法律に依存	●運転手に依存	–	○運転手に依存	–	○ 運転手への配慮に依存	● 運転手に依存	○ 運転手への配慮に依存	● 運転手に依存	○運転手に依存	○ 法律に依存	○ 運転手に依存
B3-1-1	状態の場合報酬(3.5.4.2) ・行動回避が無まる。(1.2)	CAST6-2	コントロール	UCA	競合	行動回避	–	○運転手に依存	–	–	● 設計不備	○ 運転手への配慮に依存	● 運転手に依存	○ 安全リスク評価・冗長性に依存	○ 運転手に依存	● 法律に依存	● 運転手に依存	
B3-1-2	(1-2) ・自転車の思りを誘発するためのADSモーションプラン(0.3秒前に加速)ができなくり、状況や危険(緊急事態)になる。 歩行者との衝突が迫っている時間。緊急事態を検知した。 ・行動回避が無まる。	CAST6-3	コントロール	プロセス/メンタルモデル	オペレーター	行動回避	–	○運転手に依存	–	● カメラ検出に依存	○ カメラ検出に依存	○ 運転への配慮に依存	○運転手に依存	○ カメラ検出に依存	● カメラ検出に依存	○ 法律に依存	● 運転手に依存	–
B3-1-3	(1-1)車両内部のオペレーション、システムの操作を監視。運転環境を監視し、必要に応じて車両の制御を取り、緊急時に介入することに依存を負った。(1.5.5)	CAST6-4	コントロール	車両決定状況・背景	オペレーター		–	●運転手に依存	–	–	–	–	●運転手に依存		○運転手に依存			○運転手に依存
B4	車両制御の実現無は作るの技術を確立して、運転手の操作が必要(1.5.7.3.0)に記載。 (1.4.5.3 オペレータプロフ 2.6)	CAST6-2	コントロール	UCA	対象物の制御	運転手の位置づけ	○ 運転手に依存	● 運転手に依存	–	–	○ 運転手に依存	○ 運転手への配慮に依存	○ 運転手に依存	○ 運転手に依存				○ 運転手の期待に依存
B5	行動回避の実現に伴い十分に認識できない、もしくは停車できない	CAST6-2	コントロール	UCA	対象物の制御	自動運転による行動回避	○ 設計不備	○ 設計不備	–	–	● 設計不備	○ 設計不備	○ 設計不備	● 設計不備		○ 法律に依存	● 法律に依存	● 法律の形態化に依存
B8	行動回避を計算しなかった	CAST6-2	コントロール	UCA	対象物の制御	自動運転による行動回避	○ 設計不備	–	–	–	● 設計不備	○ 設計不備	○ 設計不備	● 設計不備		○ 法律に依存	● 法律に依存	● 法律の形態化に依存
B9	急ブレーキが必要な時に運転手に警報を鳴らしていない	CAST6-2	コントロール	UCA	対象物の制御	運転手の位置づけ	–	○ 緊急時の警報に依存	–		● 緊急時の警報に依存	○ 運転手に依存	● 運転手に依存	● 運転手に依存				○ 運転手の期待に依存
B10	緊急ブレーキの必要時、緊張警報が鳴っていない。(1.5.6.1)	CAST6-2	コントロール	UCA	対象物の制御	運転手の位置づけ	–	○ 緊急時の警報に依存	–		● 緊急時の警報に依存	● 緊急時の警報不足	● 運転手に依存	● 緊急時の警報不足				○ 運転手の期待に依存
B12	ドライバーが介入が可能な情報を有用に、ADSを作設定した。(1.5.7)	CAST6-2	ADS制御	UCA	対象物の制御	運転手の位置づけ	–	● 運転手に依存	–		○ 緊急時の警報不足	● 運転手に依存	● 緊急時の警報不足					○ 運転手の期待に依存
B13	衝突回避時、運転手に警告がなかった。(1.5.5.3)	CAST6-2	ADS制御	UCA	対象物の制御	運転手の位置づけ	–	○ 緊急時の警報に依存	–		● 緊急時の警報不足	● 運転手に依存	● 緊急時の警報不足					○ 運転手の期待に依存
B4	異常検出時に運転手への警告(アへの配慮が定(1.8.3 オペレータ訓練)	CAST6-3	コントロール	プロセス/メンタルモデル	対象物の制御	運転手の位置づけ	○ 運転手に依存	● 運転手に依存	–	–	○ 運転手に依存	○ 運転手への配慮に依存	● 運転手に依存	○ 運転手への配慮に依存	● 運転手に依存	○ 運転手への配慮に依存	○ 運転手への配慮に依存	○ 運転手の期待に依存
B6	・システムの回避を想念して、行動回避を実施する設計。	CAST6-3	コントロール	プロセス/メンタルモデル	対象物の制御	自動運転による行動回避	–	○ 設計不備	–	–	● 設計不備	○ 設計不備	● 運転手に依存	● 設計不備	● 設計不備	○ 運転手への配慮に依存	○ 運転手への配慮に依存	○ 運転手の期待に依存
B8	運転手が意向を制御する間、ADS が制動を回避（１秒間）する設計(1.5.5.3)	CAST6-3	コントロール	プロセス/メンタルモデル	対象物の制御	自動運転による行動回避	–	○ 設計不備	–	–	● 設計不備	○ 設計不備	● 運転手に依存	● 設計不備	● 設計不備	○ 運転手への配慮に依存	○ 運転手への配慮に依存	○ 運転手の期待に依存
B9	・システムは車両にADSが制御中であることを運転手に警告ために、運転手に制限された。 (1.5.7 ヒューマンマシンインターフェイス)	CAST6-3	コントロール	プロセス/メンタルモデル	対象物の制御	運転手の位置づけ	○ 運転手に依存	● 運転手に依存	–	–	○ 運転手に依存	○ 運転手への配慮に依存	● 運転手に依存	● 運転手に依存	● 運転手に依存	○ 運転手への配慮に依存	○ 運転手への配慮に依存	○ 運転手の期待に依存
B10	他々に認識を開始しながら、運転手に衝突的警告を送る設計(1.5.5.3)	CAST6-3	コントロール	車両決定状況・背景	対象物の制御	運転手の位置づけ	–	○ 設計不備	–	–	● 設計不備	○ 運転手に依存	● 運転手に依存	● 運転手に依存	● 運転手に依存	○ 運転手への配慮に依存	○ 運転手への配慮に依存	○ 運転手の期待に依存
B12	HMI はタブレット上でオペレータの入力を必要とする情報を一切表示しなかった。(1.5.7)	CAST6-3	HMI	プロセス/メンタルモデル	対象物の制御	自動運転による行動回避	–	○ 設計不備	–	–	● 設計不備	○ 運転手に依存	● 運転手に依存	● 運転手に依存	● 運転手に依存	○ 運転手への配慮に依存	○ 運転手への配慮に依存	○ 運転手の期待に依存
B13	緊急時に運転手が意向を制御する設計(1.5.5.3)	CAST6-3	ADS制御	プロセス/メンタルモデル	対象物の制御	運転手の位置づけ	–	○ 設計不備	–	–	● 設計不備	○ 運転手に依存	● 運転手に依存	● 運転手に依存	● 運転手に依存	○ 運転手への配慮に依存	○ 運転手への配慮に依存	○ 運転手の期待に依存
B4	運転手は、ハンドルの上に手を乗せて座り、アレーキペダルの上に足を乗せる前提の設計(1.8.3 オペレータ訓練)	CAST6-4	コントロール	車両決定状況・背景	対象物の制御	運転手の位置づけ	–	○ 設計不備	–	○ 運転手に依存	● 運転手に依存	○ 運転手に依存	● 運転手に依存	○ 運転手に依存	● 運転手に依存	○ 運転手への配慮に依存	○ 運転手への配慮に依存	○ 運転手の期待に依存
B6	新大容時制動で衝突を回避できない場合は、車両の運転手に警告で警告し、車両の操作を開始する設計。	CAST6-4	コントロール	車両決定状況・背景	対象物の制御	運転手の位置づけ	○ 運転手に依存	● 運転手に依存	–	–	● 運転手に依存	● 運転手に依存	● 運転手に依存	● 運転手に依存	● 運転手に依存	○ 運転手への配慮に依存	○ 運転手への配慮に依存	○ 運転手の期待に依存
B8	安全の欠落性がない設計であった。	CAST6-4	コントロール	車両決定状況・背景	対象物の制御	安全への欠責性	○ 設計不備	● 運転手に依存	–	–	● 設計不備	○ 設計不備	● 運転手に依存	● 設計不備		○ 運転手への配慮に依存	○ 運転手への配慮に依存	○ 運転手の期待に依存
B9	運転手と車両間での(1)に記載不足があった。(2.2.2.1)	CAST6-4	コントロール	車両決定状況・背景	対象物の制御	運転手の位置づけ	○ 設計不備	● 運転手に依存	–	–	● 設計不備	○ 設計不備	● 運転手に依存	○ 設計不備	● 運転手に依存	○ 運転手への配慮に依存	○ 運転手への配慮に依存	○ 運転手の期待に依存
B10	自動による危険回避、緊急アレーキ時、危険な動きの変化なしに戻らから動きを維持するよう、車両回避する設計 (1.5.5.3)	CAST6-4	コントロール	車両決定状況・背景	対象物の制御	自動運転による行動回避	○ 設計不備	–	–	–	● 設計不備	○ 設計不備	○ 運転手に依存	● 設計不備		○ 運転手への配慮に依存	○ 運転手への配慮に依存	○ 運転手の期待に依存
B12	運転手は、システムの挙動、運転環境を監視し、緊急時に介入することに依存を負った。(1.5.1)	CAST6-4	ADS制御	車両決定状況・背景	対象物の制御	運転手の位置づけ	–	● 運転手に依存	–		● 設計不備	● 運転手に依存				○ 運転手への配慮に依存	○ 運転手への配慮に依存	
B13	回避の責任を有した(1.5.5.3)	CAST6-4	ADS制御	車両決定状況・背景	対象物の制御	自動運転による行動回避	–	○ 運転手に依存	–		● 設計不備	○ 設計不備		● 設計不備				
B15-1	(1-1)ADASを検出していた	CAST6-2	ADAS	UCA	対象物の制御	物体の検知化	–	● ATGの判断	–	○ ADASはよめられた物	–	○ ADASをよめた		○ ADASをよめた			● ATGの判断	–
B15-2	(1-1)レーダーの誤動作に関する検証ができていない？	CAST6-3	ADAS	プロセス/メンタルモデル	車両不足	–	–	● ATGの判断	–	○ ADASはよめられた物	–	○ ADASをよめた		○ ADASをよめた			● ATGの判断	–
B15-3	(1-2)ブレーキコマンド受信時の優先順位が設計されていない	CAST6-3	ADAS	プロセス/メンタルモデル	対象物の制御	設計不備	–	● ATGの判断	–	○ ADASはよめられた物	–	○ ADASをよめた		○ ADASをよめた			● ATGの判断	–
B15-4	(1-1)ADASを採用しようとした場合、開発に時間がかかると考えられていた？	CAST6-3	ADAS	プロセス/メンタルモデル	対象物の制御	車両不足	–	● ATGの判断	–	○ ADASはよめられた物	–	○ ADASをよめた		○ ADASをよめた			● ATGの判断	–
B15-5	(1-1)ボルボとATGシステムのレーダーが同じ周波数で作動するため、誤動作すると考えていた	CAST6-4	ADAS	車両決定状況・背景	対象物の制御	車両不足	–	● ATGの判断	–	○ ADASはよめられた物	–	○ ADASをよめた		○ ADASをよめた			● ATGの判断	–
B15-6	(1-2)ボルボAEBとATG ADSの両方からブレーキコマンドを受信した場合、正しく動作しないと考えていた。	CAST6-4	ADAS	車両決定状況・背景	対象物の制御	車両不足	–	● ATGの判断	–	○ ADASはよめられた物	–	○ ADASをよめた		○ ADASをよめた			● ATGの判断	–
	ドライバが歩行者に油断を守れるようにしていない	CAST6-2	運転、歩行者 フェンス等のない車道、見えない問題	UCA	–	–	–	●	–	–	–						●	○
	ドライバが歩行者に油断を守れるようにしていない	CAST6-2	NTSB（米国運輸安全委員会） NHTSA（米高速道路交通安全局） SAE（自自動車技術者協会） ATG（先端技術グループ(Uber)） 歩行者、ドライバー	UCA	–	–	●	–	–	–	–						●	○
	歩行者が間違を見て守る前提となっている	CAST6-3	運転、歩行者 フェンス等のない車道、見えない問題	プロセス/メンタルモデル	–	–	–	●	–	–	–						●	○
	歩行者が間違を見て守る前提となっている	CAST6-3	NTSB（米国運輸安全委員会） NHTSA（米高速道路交通安全局） SAE（自自動車技術者協会） ATG（先端技術グループ(Uber)） 歩行者、ドライバー	プロセス/メンタルモデル	–	–	●	–	–	–	–						●	○
	歩行者が車道に入ってこない前提となっている	CAST6-3	NTSB（米国運輸安全委員会） NHTSA（米高速道路交通安全局） SAE（自自動車技術者協会） ATG（先端技術グループ(Uber)） 歩行者、ドライバー	プロセス/メンタルモデル	–	–	●	–	–	–	–						●	○
	歩行者が法律に遵守する	CAST6-2	NTSB（米国運輸安全委員会） NHTSA（米高速道路交通安全局） SAE（自自動車技術者協会） ATG（先端技術グループ(Uber)） 歩行者、ドライバー	UCA	–	–	–	●	–	–	–						●	○
	異常者の行動を前提にしていない	CAST6-3	NTSB（米国運輸安全委員会） NHTSA（米高速道路交通安全局） SAE（自自動車技術者協会） ATG（先端技術グループ(Uber)） 歩行者、ドライバー	プロセス/メンタルモデル	–	–	–	●	–	–	–						●	○
	NHTSA（米高速道路交通安全局）SAE（自自動車技術者協会）ATG（先端技術グループ(Uber)）がドライバーに警告する仕組みを準備しない	CAST6-2	NTSB（米国運輸安全委員会） NHTSA（米高速道路交通安全局） SAE（自自動車技術者協会） ATG（先端技術グループ(Uber)） 歩行者、ドライバー	UCA	–	○	–	●	–	–	–						●	○
	「ドライバーが正しく運転する前提になっている	CAST6-3	NTSB（米国運輸安全委員会） NHTSA（米高速道路交通安全局） SAE（自自動車技術者協会） ATG（先端技術グループ(Uber)） 歩行者、ドライバー	プロセス/メンタルモデル	–	○	–	●	–	–	–						●	○
	公衆としての安全管理の責務を組織として行っていない 安全リスクマネジメントが行われていない	CAST6-2	ATG（先端技術グループ(Uber)）	UCA	–	–	–	–	○	–	–					○	●	
	安全管理体制が甘い 従来の安全文化・方針逸脱を確認しない	CAST6-3	ATG（先端技術グループ(Uber)）	プロセス/メンタルモデル	–	–	–	○	–	–	–						●	
	従業員が遵守すべき指示業務事項の確認行為を行っていない	CAST6-2	ATG（先端技術グループ(Uber)） ドライバー	UCA	–	–	–	○	–	–	–					○	●	
	関係運行確認の欠如	CAST6-3	ATG（先端技術グループ(Uber)） ドライバー	プロセス/メンタルモデル	–	–	○	–	–	–	–					○	●	
	従業員の遵守状況の報告が行われていない	CAST6-2	ATG（先端技術グループ(Uber)） ドライバー	UCA	–	–	–	○	–	–	–						●	
	安全保証の基準の設定なし	CAST6-3	ATG（先端技術グループ(Uber)） ドライバー	プロセス/メンタルモデル	–	–	○	–	–	–	–					○	●	
	従業員の事務運転時の監視を行っていない	CAST6-2	ATG（先端技術グループ(Uber)） ドライバー	UCA	–	–	●	–	–	–	–						●	
	運転者の異常検知とフィードバックが不十分	CAST6-3	ATG（先端技術グループ(Uber)） ドライバー	プロセス/メンタルモデル	–	–	●	–	–	–	–					○	●	
	飲酒運転の試験を行う企業に対する統制行為の対象が（リスクに対応して）網羅されていない	CAST6-3	アリゾナ州 ATG（先端技術グループ(Uber)）	UCA	–	–	○	–	–	–	–					●		○
	当該事項に対するリスク分析と対策が不十分	CAST6-3	アリゾナ州 ATG（先端技術グループ(Uber)）	プロセス/メンタルモデル	–	–	–	–	–	–	–					●		○
	飲酒運転に関する 安全当点た評価プロセスが不十分 ・安全基準の策定 ・当該評価の試験手順の提示 が当他的でない	CAST6-2	NTSB（米国運輸安全委員会） NHTSA（米高速道路交通安全局）	UCA	–	○	–	–	–	–	–					●		
	「部分的」としているものの、対象者が宣告的に対処できるような行動指針・遵守レベルが不明瞭から示されていない	CAST6-3	NTSB（米国運輸安全委員会） NHTSA（米高速道路交通安全局）	プロセス/メンタルモデル	–	–	○	–	–	–	–					●		○
	AAMVAの適用のオペレーションと事業者に対して飲酒運転や安全対策に対する統制に関与していない	CAST6-2	AAMVA	UCA	–	–	○	–	–	–	–					●		○
	飲酒運転者と安全対策へのアプローチがプロセスされていない？(各州間の連携含め)	CAST6-3	AAMVA	プロセス/メンタルモデル	–	–	○	–	–	–	–					●		○
	飲酒運転システムに対する安全基準や課題の仕組みがない	CAST6-2	NTSB（米国運輸安全委員会） NHTSA（米高速道路交通安全局）	UCA	–	○	–	–	–	–	–					●		○
	飲酒運転システムに対する安全基準や課題をどう扱り扱うかのプロセスがない？	CAST6-3	NTSB（米国運輸安全委員会） NHTSA（米高速道路交通安全局）	プロセス/メンタルモデル	–	○	–	–	–	–	–					●		○
	ドライバーが状況を把握しようとしていない（安全義務を放棄している）	CAST6-2	ドライバー	UCA	–	○	●	–	–	–	–					○	●	○
	飲酒運転車両でのドライバーの義務を全うしていない	CAST6-3	ドライバー	プロセス/メンタルモデル	–	○	●	–	–	–	–					○	●	○
	運転に集中していない	CAST6-2	ドライバー	UCA	–	○	●	–	–	–	–					○	●	○
	飲酒運転車両とドライバーの義務が理解になっている。	CAST6-3	ドライバー	プロセス/メンタルモデル	–	○	●	–	–	–	–					○	●	○

付録8_表5：事例の特徴と分析から見える弱点とその改善案

項	特徴	分析から見える弱点	改善勧告案
1	法律に関するもの	歩行者が交通ルールを守ることが前提、横断歩道以外の道路上では車両が優位になる	今までの運転者と歩行者の関係であれば、人対人になり、現状のルールでも可能かもしれない 自動運転になると人対システム対人となり、現状のルールでは対応できない 自動運転時の運転者の状態を管理、監視する機能の義務化などの法整備と自動運転自動車対歩行者の法律上の定義が必要
2		横断禁止のルールはあるが、標識のみでは効果が薄い	標識による注意喚起は、通常の歩行者には有効だが、何らかの異常状態になっていると判断できない 通常の運転手であれば、気づけたかもしれないが自動運転では認識処理ができないことがある 横断を禁止するのであれば、柵をつけるなど、物理的な対策が必要
3		歩行者の薬物摂取、飲酒等の外的要因により判断できない状況が考慮されていない	何らかの薬物等の摂取について、適法か合法かは別の法律になる 国、州によって薬物の法律には違いがある 歩行者の認識が正常にできない状態であっても、誤って道路を横断している歩行者を、検出して対応できる認識能力が自動運転に必要となる 法律による一律の例外、除外は自動運転システムが危険な状態になる
4		自動運転では今までの運転免許だけでは十分ではない	自動運転時の運転手の不注意について法整備が必要 運転中は前方を注視、回避可能な状態を維持するか、自動運転システムの認証制度により、人間の目視による判断と自動運転システムに差分がないことを条件とする 何らかの自動運転システムの認証が必要
5		自動運転に関する連邦安全基準がない。 新技術のシステムに対して、国家・政府レベルでの安全管理の監督活動や評価を行う仕組みがない。	自動運転に関する連邦安全基準を定め、国家・政府レベルでの安全管理の監督活動を行う。 もしくは、新技術といったリスクが不透明な事案に対しては、安全基準やリスク評価を具体的に検討するための体制を構築することをプロセスとして定める。
6	人に関するもの	交通ルールの欠如（歩行者） 以下の交通ルールに従っていなかったため車両から正しく検出されず、衝突事故にあったと考えられる。 － 交通管制信号機が作動している隣接する交差点間では、歩行者は標示された横断歩道以外の場所を渡ってはならない。 － 道を横断する歩行者は、標識のある横断歩道または交差点の標識のない横断歩道以外の場所で車道を横断する場合は、車道を走行するすべての車両に道を譲らなければならない。	歩行者に対し、交通ルールを徹底する教育が必要
7		メンテナンスの形骸化（歩行者） 自転車のライトが前方を照射していなかったことで、自動車からの発見が遅れた可能性があり、自転車のメンテナンスが不十分であったと考えられる。	自転車のメンテナンスに関する仕組みづくりが必要。
8		注意力の欠如（運転手） 運転手がシステムの操作の監視、運転環境の監視を怠ったことで緊急時の車両の制御ができなかったと考える。具体的には以下への注意が必要だった。 － ADSが解除されたことに関する通知 － 運転環境	車両の運転手が注意を払っていれば、衝突を回避したり、衝撃を緩和したりするために、横断する歩行者を検知して反応するのに十分な時間があった可能性が高い。 車両の試験の場合は、オペレータを2人以上とし、システムや運転環境の監視のみならず、ドライバーの監視を行う仕組みを組み込む
9		異常行動は制御できない	人がルールを守らないことに対する措置を行う（前提により対応が異なる） ＜守る前提＞歩行者の法律違反による事故は、車両側の過失責任なし。 ＜守らない前提＞ドライバの安全義務負荷を下げる工夫をする。 －物理的対応（フェンス等） －警告（電光掲示板、車内警告 等）
10		「人はルールを守る」ことが前提となっている	
11		自動化が進むほど、人の安全に対する意識はなくなる。	自動運転試験に関係ないステークホルダを巻き込む可能性のある場所での試験を禁止する。
12	周辺機器に関するもの	・スペックの検討不足（カメラ） 障害物を検出するカメラのスペックが低く、人間であれば検出できる対象物がカメラでは検出できていなかった可能性がある。	物体検出用に搭載するカメラ、センサーのスペックについて十分な検証を行い、基準を制定する必要がある
13		・警報に関する検討不足 警報を鳴らすのはソフトウェアであり、警報機については不具合がなかったと思われるため、記載なし	ユーザーへの通知 ADSを解除した理由をドライバーに通知する仕組みを組み込む。 特にシステム障害により解除した場合は通知が必須。 例：解除理由をディスプレイに文字列とディスプレイの色で表示する
14		・ドライバーとのコミュニケーションの欠如（HMI） ADSを解除した際に解除した理由をドライバーに通知する仕組みが必要だったと考える。	再設定の制限 システム障害により解除した場合は障害の原因を取り除くまでドライバーによる再設定ができなくなるような仕組みを組み込む。
15	設計に関するもの	安全性、リスクに対する評価・冗長性への配慮不足 ・基本的には、州の交通法に基づいた（依存した）設計がなされているが、「交通ルールを守らない対象物が路上にはある」といったこと等への配慮が全体的に不足していると考える。	対象物について「交通ルールが遵守されない」ことに対するリスク検討・安全性向上に向けた冗長的なロジック検討し追加することで事故を回避できる可能性がある。 （知覚／予測コンポーネントだけでなく、コントロール、ADS制御等のコンポーネントに対してもロジック等の追加が必要）
16		・車両と運転手とのインターフェースについては緊急時には運転手の判断に基づく（依存した）設計がなされているが、「運転手は不安全な運転を行う」といったこと等への配慮が全体的に不足していると考える。	緊急時には、とっさの行動が運転手にはできない可能性があることを前提とし、「緊急時に自動運転が行う最低限度の安全確保の行動」を定義することで事故の回避／衝突ダメージを低減できる可能性がある。
17		・車両と運転手とのインターフェースの一つに「警報」の仕組みを用いている （依存した）設計がなされているが、「運転手は警報を無視する（誤報含む）／警報を切る」といったこと等への配慮が全体的に不足していると考える。	「警報」に依存した設計とする場合は、「警報無視」、「警報切」による運転手の不安全行動への対応として、自動で車両停止等による安全性確保に向けた冗長的な仕組みを検討し追加することで事故を回避できる可能性がある。
18		急動作への対応について（安全性の高い車両コントロールへの配慮不足） ・後続車両への配慮、運転手による誤った急動作（アクセルとブレーキの踏み間違い等）への配慮により「衝突を防ぐための急制動が必要な場合には、1秒間制動を抑制するように設計された」ことで、減速されない状況で事故が発生している。	「衝突を防ぐための急制動」は運転手による依存ではなく、自動制動を実施することで回避／衝突ダメージを低減できる可能性がある。 またカメラ、センサの種別、機能、精度向上等による対応を組合わせることで、早期の検出・回避ができる可能性がある。
19		対象物に対する知覚ロジック／予測ロジックについての配慮不足 ・「知覚に関するコンポーネント」⇔「予測に関するコンポーネント」の機能連携等の配慮が不足していると考える。 【補足事項】 「対象物の分類・再分類に対する変更管理」、「対象物の分類変更があった際、それまでの履歴を利用しない仕様」等、「知覚に関するコンポーネント」⇔「予測に関するコンポーネント」の連携を指す。	「知覚に関するコンポーネント」⇔「予測に関するコンポーネント」の機能連携等の機能拡充を行うことで、事故を回避することができる可能性がある。 （知覚／予測コンポーネントだけでなく、コントロール、ADS制御等のコンポーネント類の連携に対しても機能拡充が必要）
20		・「走行車線で検出された対象物」でかつ、「車両として分類された物体」について、「一般的にその車線の交通方向への走行目標が割り当てられる」設計仕様としたことで、「歩行者」、「自転車」等に知覚ロジック、予測ロジックすることへの配慮が不足していると考える。 【補足事項】 州の交通法に依存した「対象物は交通ルールを守る」ことを前提とした設計内容であったが、対象物について「交通ルールが遵守されない」ことに対するリスク検討・安全性向上に向けた冗長的なロジック検討の配慮不足。	対象物について「交通ルールが遵守されない」ことに対するリスク検討・安全性向上に向けた冗長的なロジック検討し追加することで事故を回避できる可能性がある。 （知覚／予測コンポーネントだけでなく、コントロール、ADS制御等のコンポーネントに対してもロジック等の追加が必要）
21		・知覚ロジックにて利用するカメラ、センサの種別、機能、精度への配慮が不足していると考えられる。（映像系のセンサに依存した設計であること） 【補足事項】 事故報告書には熱源感知センサ、音声感知センサの利用等についての記載がないため、利用されていないと考える。	今回の事故事例は車両や人通りの少ない夜の郊外道路で発生した事故であり他のセンサ類の情報を組合わせることで事故を回避できる可能性がある。
22	企業の安全文化・マネジメントシステムに関するもの	企業として安全文化・方針の浸透、安全管理業務・安全リスクマネジメントを行う組織がなく、安全管理者の任務が確実に行われていることが確認できない	企業としての安全管理業務および安全リスクマネジメントを行う専任組織を設置し、安全管理と安全リスクマネジメントの確実な実施を図るとともに、安全管理が確実に実施されていることを確認する
23		雇用開始時、または定期的に、従業員に対して遵守すべき重要事項の確認行為を行っていない 随時・定期的等タイミングを設けて、遵守状況の監査を行っていない 自動運転時の不遵守状況が適切に監視されていない	遵守すべき重要事項は、適切なタイミング（従事時、または定期）で検査・監査を行い遵守状況を確認する。
24	ステークホルダに関するもの（州、AAMVA、連邦）	州から企業に対する統制が不十分	州として ・企業に対して、安全性の監督と統制を行う体制、仕組みを構築し適用させる ・体制や仕組みを構築する以前に不透明な場合でも、州としてリスク評価を行う体制を構築する
25		自動運転の安全性に関する方針は示しているが、 開発者が行うべき安全性自己評価プロセスが不十分 安全基準の策定、性能評価の試験手順の提示が具体的でなく、 具体的な実施基準・評価の仕組みとして示されていない	連邦レベルで安全性自己評価プロセスと実施基準を定め、行うべき対象者に実施を義務付ける
26		国及び地方自治体の職員を代表する団体であり、管理、法執行、モデルプログラム開発を開発。高速道路の安全問題のための情報交換所としての役割を果たしているが、 新しい技術が出る文脈では関わりが不透明。 他の州からの情報を踏まえて法整備等プロセスに関与していない、州への統制不十分	連邦のすべての州が事業者に対して、新技術を含む安全対策に対する統制が図れるよう、各州との情報連携を行い、安全管理の法やモデルプログラムを浸透させる。そのための体制を構築する。

付録9_表6：コンポーネント抽出表

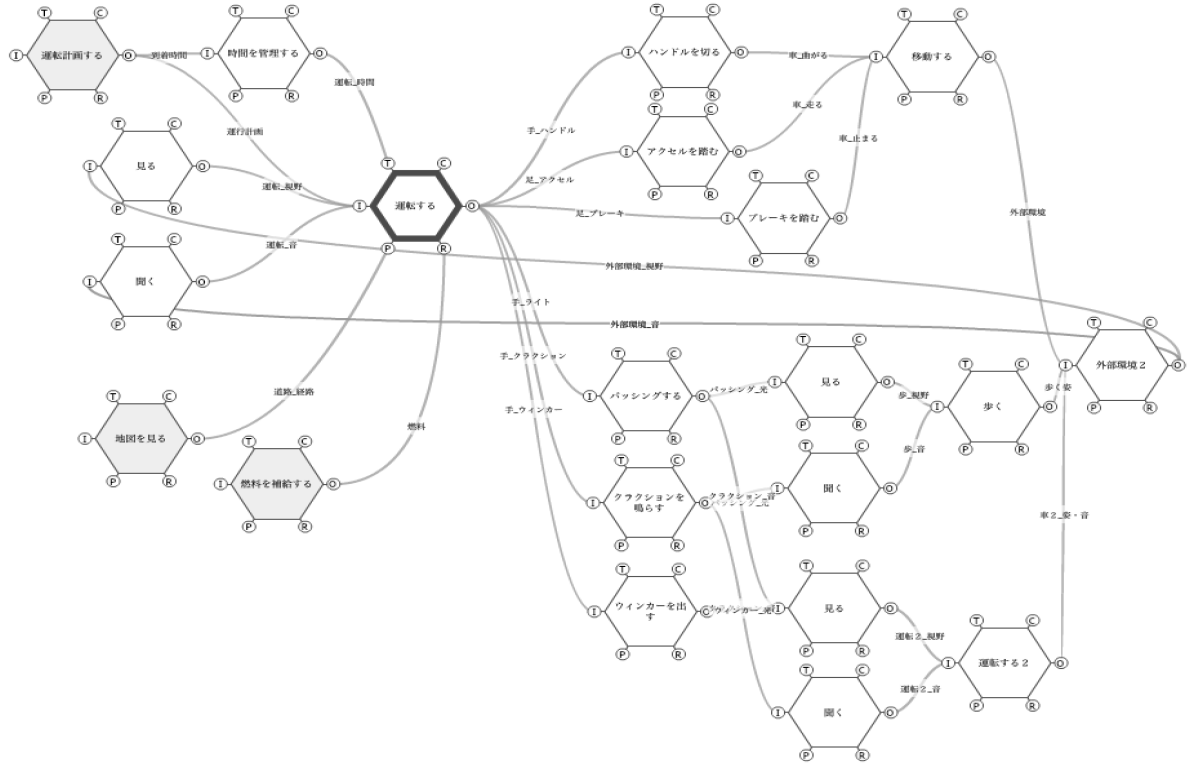
対象	登場人物	責務	コントロールアクション	フィードバック	入出力	備考
true	通行人・他自動車	交通ルールの遵守	認識 (To: 自動車)			
true	目的地	たどり着くべき場所		なし		
true	貨物	品質を保ち目的地に到着				
true	同乗者	健康状態を保ち目的地に到着				
true	自動車	安全に交通ルールを守り目的地へ到着する				
true	センサー （超音波センサー）	低速域で距離を認識	認識 (To: 外界情報)			
true	センサー （赤外線センサー）	センサーで人を認識	認識 (To: 外界情報)			
true	センサー （ミリ波レーダミリ波レーダ）	悪天候や暗さを認識	認識 (To: 外界情報)			
true	センサー （GPSセンサー）	自己位置の推定	認識 (To: 外界情報)			
true	センサー （加速度・ジャイロセンサ）	GPSやその他のセンサの信号が正しく取得できない場合、自己位置の推定	認識 (To: 外界情報)			
true	カメラ （ステレオカメラ）	車間距離や相対速度を計測	認識 (To: 外界情報)			
true	カメラ （単眼カメラ）	後方や側方の視覚を計測認識 駐車支援のアラウンドモニターを計測 車線維持を目的とした白線認識 交通標識の認識 横断歩道（道路標示/規制表示）の認識	認識 (To: 外界情報)			
true	ドライバ監視カメラ	ドライバの不自然な動作を認識	認識 (To: 運転者)			
true	ライダー （周辺の物体の検出＝自車位置、周辺の物体の検出）	物体までの距離や方向を測定	認識 (To: 外界情報)			
true	ライト	パッシングを行い、意思を伝える	パッシングする (To: 通行人・他自動車) 点灯・消灯 (To: 自動車)			
true	ワイパー	視界を良好に保つ	動かす (To: 運転者) 動かす (To: AI)			
true	ウインカー	移動方向を伝える	動かす (To: 運転者) 動かす (To: AI)			
true	ブレーキ	徐々にスピードを落とし安全に停止する	かける (To: 運転者) かける (To: AI)			
true	アクセル	徐々にスピードを加速し安全に走行する	踏む (To: 運転者) 踏む (To: AI)			
true	ネットワークシステム	運転に必要な多数の情報を取得・出力する	アクセスする (To: AI)			
true	サイバーセキュリティ	サイバー攻撃による妨害・迷惑行為を受けない	装備 (To: 自動車)			
true	ソフトウェア（アップデート）	情報を最新化し脆弱性を持たないようにする	装備 (To: 自動車)			
true	作動状況記録装置	記録を人の視覚又は聴覚により認識することができる状態にする	装備 (To: 自動車)			
true	電源系統	電源ネットワーク（パワーネット）の冗長性	装備 (To: 自動車)			
true	ドライブレコーダー		録画 (To: 外界情報) 録画 (To: 運転者)			
true	EDR		録画 (To: 外界情報)			
true	OBD		チェック (To: 自動車)			
true	ディープラーニング	正しい認識を行うことができるように学習する	学習する (To: AI)			
true	AI	情報を基に予測を行い、適切な判断を下す	判断・予測・行動計画 (To: センサー系・カメラ系)			
true	クラクション	クラクションを鳴らし意思を伝える	鳴らす (To: 通行人・他自動車)			
true	外界情報					
false	運転者					レベル0項目のため除外
false	運転者（目視）	通行人・他車・障害物・車間距離等を認識	認識 (To: 外界情報)			同上
false	運転者（聴覚）	遮断機・クラクション・救急車サイレン等の音を聞く	認識 (To: 外界情報)			同上
false	運転者（嗅覚）	異臭よる異常を感知	認識 (To: 外界情報)			同上
false	運転者（体感）	振動による異常を感知	認識 (To: 自動車)			同上
false	運転者（思考）	情報を基に予測・判断を行い行動する	判断 (To: 運転者（目視）) 判断 (To: 運転者（聴覚）) 判断 (To: 運転者（嗅覚）) 判断 (To: 運転者（体感）)			同上
true	センサー・カメラ・ライダー					
true	センサー（聴覚）	遮断機・クラクション・救急車サイレン等の音を聞く	認識 (To: 外界情報)			
true	センサー（嗅覚）	異臭よる異常を感知	認識 (To: 自動車)			
true	センサー（体感）	振動による異常を感知	認識 (To: 自動車)			
true	交通ルール・法律	交通ルール・法律を遵守する	遵守 (To: 自動車)			
true	カーセキュリティ	車両を盗難から守る	装備 (To: 自動車)			
true	エアコン	車内の安全・室温	装備 (To: 自動車)			
true	インフラ整備	自動運転を行う条件を満たしていること	整備 (To: 外界情報)			

付録10_表7：対策表

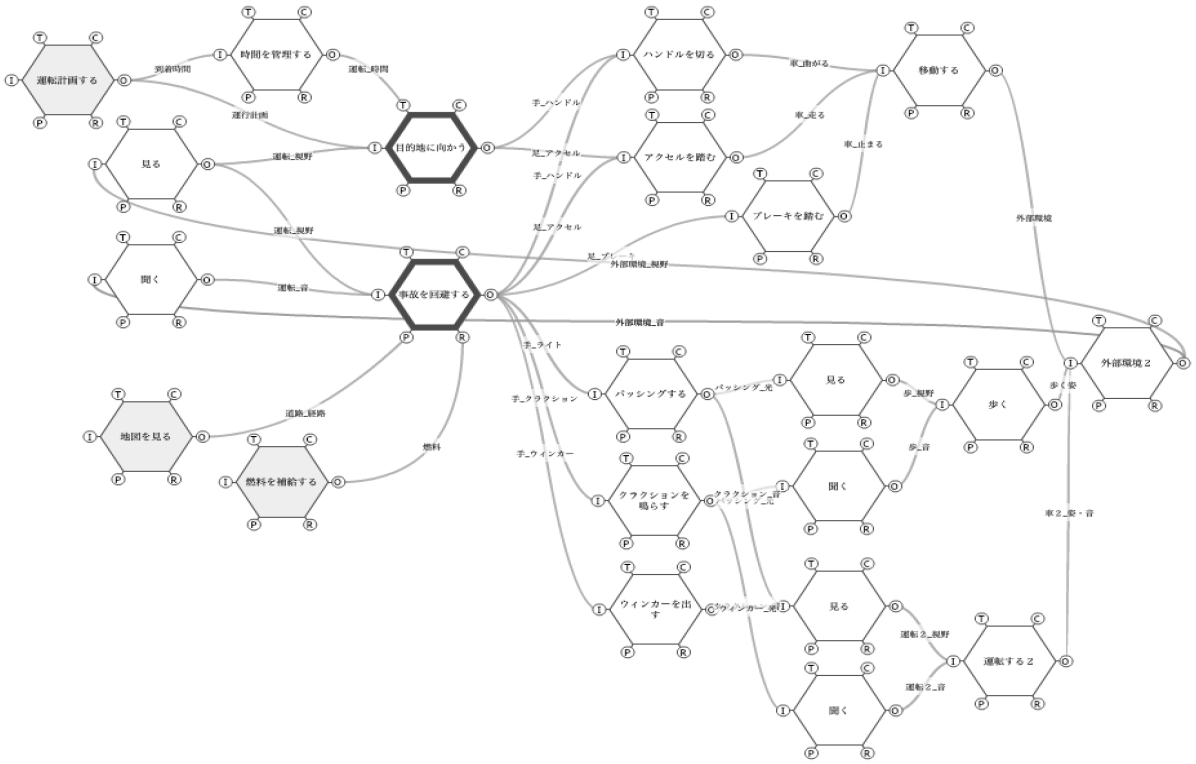
HCFID	HCF	対策ID	対策	UCA	対策対象コンポーネント	備考
HCF9-N-1-1	ADSは衝撃の5.6秒前に歩行者を検出. ADSは,衝突まで歩行者を追跡し続けが,ADSは,彼女を歩行者として正確に分類したり,彼女の経路を予測したりすることは決してなかった.	M1	衝突の2.5秒前に前方衝突警告がドライバーに警告を発したことからボルボADASでは人として検知可能.動作保証をされている赤外線センサーを起動させる	(UCA9-N-1) センサー （赤外線センサー）で人を認識できず事故を起こす [SC2]		
HCF22-N-1-1	システムは,緊急ブレーキをかけず,代わりに,車両を徐々に減速させる 計画を開始したときに,車両運転者に聴覚警報を鳴らした.	M2	Uber ADSでは警報を鳴らし始めたが運転手は間に合わなかった. レベル5では緊急ブレーキか減速開始を早めるべき.	(UCA22-N-1) ブレーキをかけるが停止することができず事故につながる [SC22]		
HCF2-N-1-1	今回のケースでは,通行人は自動車を認識することが出来ていなかった	M3	今回のケースでは,薬物が検出されており,正常な意識をもっていなかった可能性がある. そのような人物である場合は,道路に入場させない. または衝突をしても怪我などにならないように車両の素材を考慮するなどが考えられる.	(UCA2-N-1) 自動車を認識できないことにより通行人・他自動車が回避行動を行うことができない [SC38]		今回は,道路については見通しが良かったことスピードも60キロ程度,ライトも点灯している. 通常ならクラクションやパッシングでの注意喚起を自動で行うことも対応可能だと思われる.
HCF2-T-1-1	今回のケースでは,通行人は自動車を認識することが出来ていなかった	M3	今回のケースでは,薬物が検出されており,正常な意識をもっていなかった可能性がある. そのような人物である場合は,道路に入場させない. または衝突をしても怪我などにならないように車両の素材を考慮するなどが考えられる.	(UCA2-T-1) 自動車を遅すぎる認識で,車両・身体の損失または人命の損失 [SC38]		今回は,道路については見通しが良かったことスピードも60キロ程度,ライトも点灯している. 通常ならクラクションやパッシングでの注意喚起を自動で行うことも対応可能だと思われる.
HCF22-T-1-1	ブレーキによる遅すぎた減速は発生した.（ただしボルボでは20種のうち17種では回避可能だった）	M2	Uber ADSでは警報を鳴らし始めたが運転手は間に合わなかった. レベル5では緊急ブレーキか減速開始を早めるべき.	(UCA22-T-1) ブレーキによる不用意な不停止・停止により事故につながる [SC22]		
HCF22-N-1-2	ブレーキをかけたが停止することが出来ない	M2	Uber ADSでは警報を鳴らし始めたが運転手は間に合わなかった. レベル5では緊急ブレーキか減速開始を早めるべき.	(UCA22-N-1) ブレーキをかけるが停止することができず事故につながる [SC22]		
HCF25-N-1-1	自動運転レベル３報告書では学習の記載なし	M4	今後レベル5に向けて学習を繰り返し,外界情報のよる判別の精度・予測の制度をあげることに運転機能の向上となる	(UCA25-N-1)学習不足による判断ミス・予測不備よる事故・違反が起きる [SC24]		
HCF25-P-1-1	自動運転レベル３報告書では学習の記載なし	M5	今後レベル5に向けて学習を繰り返し,誤情報を取り込む可能性があるがその場合,誤情報だという認識を与える必要がある	(UCA25-P-1)間違った学習による判断ミスよる事故・違反が起きる [SC24]		
HCF26-N-1-1	自動運転レベル３報告書ではネットワークの記載なし	M6	ネットワークからの渋滞情報・災害情報の取得により渋滞の緩和,災害時の避難などに役立つと考えられる	(UCA26-N-1) ネットワークからの最新状況の不足による事故・違反が起きる [SC25]		
HCF26-P-1-1	自動運転レベル３報告書ではネットワークの記載なし	M7	ネットワーク情報が最新でないか,周辺の車両からも情報を取り込み最新化されているか確認を行う	(UCA26-P-1) ネットワークの間違った情報による判断ミスよる事故・違反が起きる [SC25]		
HCF3-N-1-1	自動運転レベル３報告書では検知しクラクションを鳴らす機能がない	M8	レベル3では,クラクションによる注意喚起は自動では行われない,それを自動で行うことに的確に注意喚起を行う	(UCA3-N-1) 通行人・他自動車へクラクションを鳴らすことにより注意・意思が伝わらず事故につながる [SC17]		
HCF3-T-1-1	自動運転レベル３報告書ではクラクションを鳴らす機能がない	M8	レベル3では,クラクションによる注意喚起は自動では行われない,それを自動で行うことに的確に注意喚起を行う	(UCA3-T-1) 通行人・他自動車へクラクションを鳴らすのが遅れたことに注意にならず事故につながる [SC17]		
HCF35-N-1-1	自動運転レベル３報告書ではサイバーセキュリティの記載なし	M9	レベル5では,IoTの乗っ取り,悪意あるアプリケーションのダウンロードを防ぐため必須	(UCA35-N-1) サイバーセキュリティが装備されていないことにより,IoT機器をのっとり,車両へ悪意のあるアプリケーションをダウンロードがされ事故・事件・盗難が起きる恐れ [SC26]		
HCF35-T-1-1	自動運転レベル３報告書ではサイバーセキュリティの記載なし	M10	対応漏れが出ないようある程度の単位で対応を行えるようにする必要がある.	(UCA35-T-1) サイバーセキュリティが装備や更新が 遅すぎるとIoT機器をのっとり,車両へ悪意のあるアプリケーションをダウンロードがされ事故・事件・盗難が起きる恐れ 保安基準を満たせず責任を問われる [SC26]		
HCF4-N-1-1	自動運転レベル３報告書ではパッシングの自動機能なし	M11	レベル3では,パッシングによる注意喚起は自動では行われない,それを自動で行うことに的確に注意喚起を行う	(UCA4-N-1) 通行人・他自動車へパッシングによる注意が伝わらず事故につながる [SC17]		
HCF4-T-1-1	自動運転レベル３報告書ではパッシングの自動機能なし	M11	レベル3では,パッシングによる注意喚起は自動では行われない,それを自動で行うことに的確に注意喚起を行う	(UCA4-T-1) 遅すぎるパッシングにより通行人・他自動車への認識が間に合わず事故につながる [SC17]		
HCF41-N-1-1	自動運転レベル３報告書では音に関わる自動機能記載なし	M12	レベル3では存在しない遮断機,クラクション,救急車,消防車等の音を認識し,停止,端によるなどの機能追加が必要	(UCA41-N-1) 遮断機・クラクション・救急車サイレン等が聞こえず事故につながる [SC32]		
HCF42-N-1-1	自動運転レベル３報告書では匂いによる自動機能なし	M13	レベル3では存在しない匂いによる故障の判別などを行える	(UCA42-N-1) 異臭よる故障に気付かない [SC33]		
HCF43-N-1-1	自動運転レベル３報告書では振動による自動検知機能の記載なし	M14	レベル3では存在しない振動やハンドルによる抵抗感による車両の異常を検知する	(UCA43-N-1) 振動による故障に気付かない 走行の安定感がない [SC34]		
HCF44-N-1-1	通行人が道路を横断しないという交通ルールを守らなかった	M15	現時点は自動運転による通行人の交通ルール改正はないが,今後通行人に対するルール追加の考慮が必要	(UCA44-N-1) 交通ルールを侵害し罪に問われる [SC36][SC38]		
HCF47-N-1-1	自動運転レベル３報告書ではインフラ整備についての記載なし	M16	レベル5の実現化において,認識の精度を高めるため標識の統一や横断歩道の追加,視覚の誤認識を起こしやすい道路の改修など,インフラ整備に関するルール決めが必要	(UCA47-N-1) インフラ整備が行われていることにより自動運転を行う上で動作が保証される [SC40]		
HCF9-N-1-2	衝突を伴うSUVにインストールされているCity Safetyのバージョンは,歩行者,自転車,または大型の動物も検出できます. システムが差し迫った衝突を検出した場合,ドライバーに警告するか,自動的にブレーキをかけます. 歩行者と自転車の検出コンポーネントは,車両が最大時速43マイルで走行しているときに,歩行者や自転車との衝突を回避または緩和できます.	M17	今回のボルボADASでは問題なし	(UCA9-N-1) センサー （赤外線センサー）で人を認識できず事故を起こす [SC2]		
HCF22-N-1-3	シミュレーションの結果,衝突の2.5秒前に前方衝突警告がドライバーに警告を発し,衝突の1.4秒前に自動緊急ブレーキ が作動することがわかりました.ドライバーが反応しなかったと仮定し,自動緊急ブレーキ の作動のみを考慮した場合,SUVは20種類の歩行者の動きのうち17種類で歩行者との衝突を回避する（85%？）と予測されました.	M18	自動運転レベル5ではそれ以上の早い段階で「自動緊急ブレーキ」が行われることにより回避が可能ではないのかと思われる. Uber ADSでも人という認識はされていないが「ADSは衝撃の5.6秒前に歩行者を検出」している.ボルボADASの「前方衝突警報」でも,衝突の2.5秒前に稼働するため,現時点の1.4秒前より開始する対策により回避が可能と思われる	(UCA22-N-1) ブレーキをかけるが停止することができず事故につながる [SC22]		
HCF10-N-1-1	警察が視認性を確認したところ,街灯が歩行者の進路を十分に照らしており,車両の運転手が歩行者の動きを検知することができたと判断 障害物は存在せず,車両の運転手は衝突の5.6秒前に歩行者と明確な視線を持っていたことになる.さらに,視線評価では,衝突するまでの間,車両の運転手は常に歩行者との明確な視線を確保していたことが示されています.	M19	今回のミリ波レーダーの機能において問題なし	(UCA10-N-1) センサー （ミリ波レーダミリ波レーダ）が悪天候や暗さの中で認識できず事故を起こす [SC3]		
HCF44-N-1-2	米高速道路交通安全局(NHTSA)は,FCW,AEB,ADSなどのシステムに必要な安全基準 を策定しておらず,最小ADS性能を評価するための試験手順を提案していない. 米国家運輸安全委員会(NTSB)は,ADSの連邦安全基準および評価プロトコルが欠如していること,ならびに 米高速道路交通安全局(NHTSA)の安全性自己評価プロセスが不十分である	M20	Uberの事故事例では,車両システム安全基準などのルールが曖昧であった. そのためレベル5においては車両システムの安全基準を明確に遵守する法律が必要	(UCA44-N-1) 交通ルールを侵害し罪に問われる [SC36][SC38]		
HCF26-T-1-1	自動運転レベル３報告書ではネットワークの記載なし	M7	ネットワーク情報が最新でないか,周辺の車両からも情報を取り込み最新化されているか確認を行う	(UCA26-T-1) ネットワーク情報のタイムラグにより最善の対応を行うことが出来ない [SC25]		

付録11_図3：FRAMモデル（1/2）

自動運転レベル０（人間が運転する場合）のFRAM図　~「運転する」機能を中心に作成~

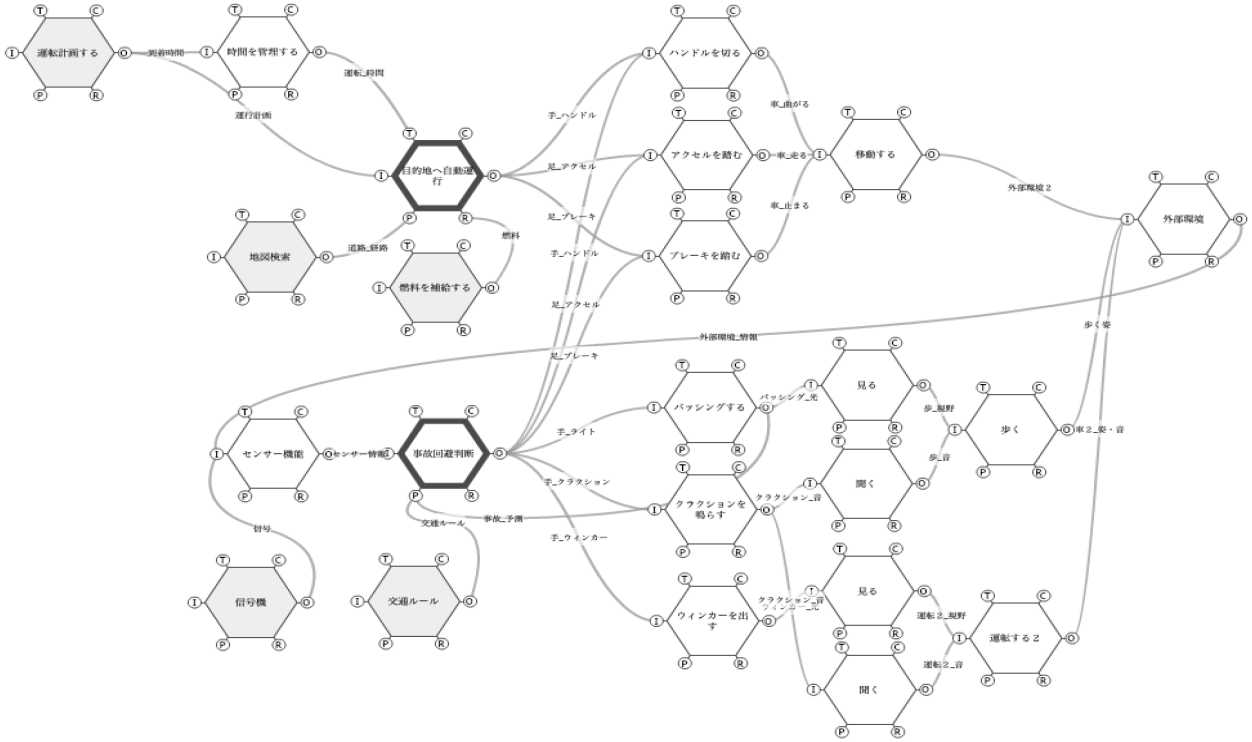


自動運転レベル０（人間が運転する場合）のFRAM図　~「運転する」機能を「目的地に向かう」「事故を回避する」機能に分解~

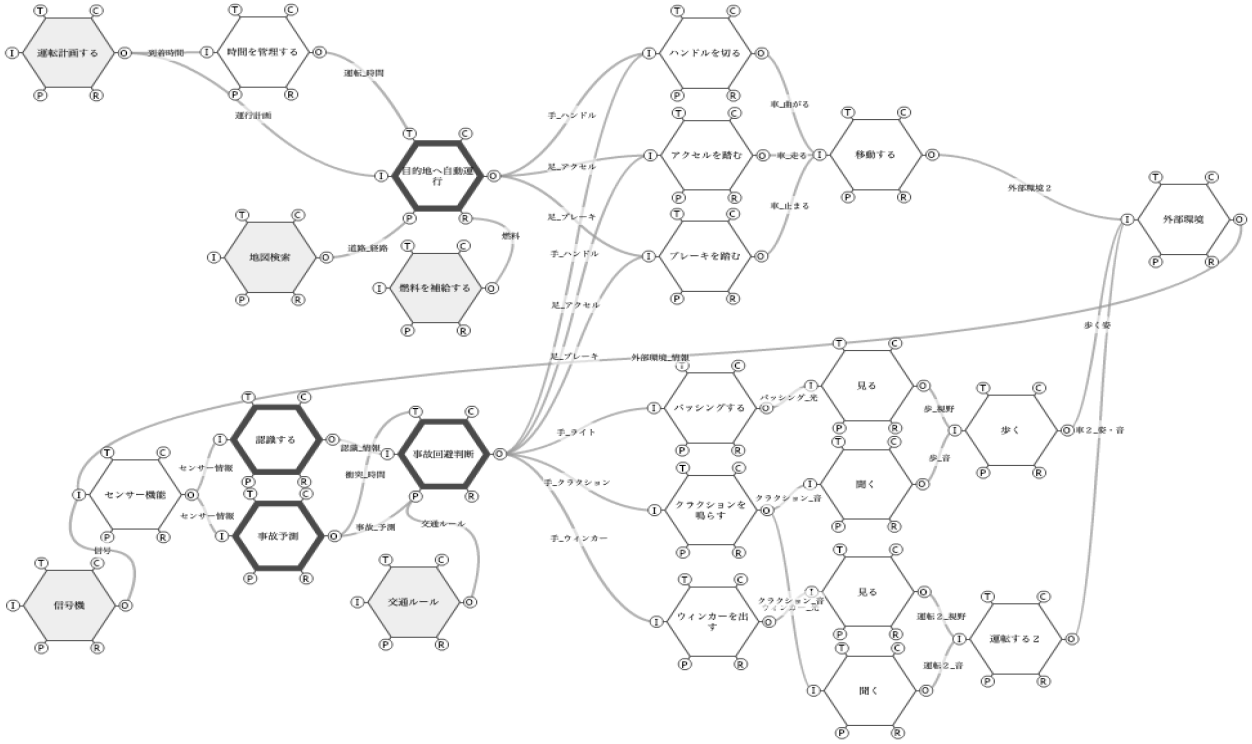


付録12_図3：FRAMモデル（2/2）

自動運転レベル5のFRAM図　~人間の運転機能を自動運転に置き換え~



自動運転レベル5のFRAM図　~「Monitor」「Anticipate」機能を追加~



付録13_事故報告書とCAST分析結果の比較（考察）

	被害を発生・拡大させた要因 （本文と連動）	再発防止のための対策（事故報告書より） 現時点で措置済みの対策	再発防止のための対策（事故報告書より） 今後取組む抜本的対策	CAST分析で新たに導き出した改善案
1	弱点１　歩行者が交通ルールを守ることが前提、横断歩道以外の道路上では車両が優位になる	近い内容はあり •ATGの安全文化が不十分である。車両運行者の監督を含む安全リスク管理手順や安全方針の不備が考慮される: ATGの安全リスク管理(セクション2.2.1)。 ・運転者による車両自動化の監督(セクション2.2.2)。 ・ATGの安全方針(安全方法、プロセス、組織構造を含む)(セクション2.2.3)。	今までの運転者と歩行者の関係であれば、入力人になり、現状のルールでも可能かもしれない 自動運転になると人対システム対人となり、現状のルールでは対応できない 自動運転時の運転者の状態を管理、監視する機能の義務化などの法整備と自動運転自動車対歩行者の法律上の定義が必要	報告書では、今回のような自動運転テストについてであり、未来の目的である５レベル５に対応するための定義が必要
2	弱点２　横断禁止のルールはあるが、標識のみでは効果が薄い	同上	標識による注意喚起は、通常の歩行者には有効だが、何らかの異常状態になっていると判断できない 通常の運転手であれば、気づけたかもしれないが自動運転では認識処理ができないことがある 横断を禁止するのであれば、柵をつけるなど、物理的な対策が必要	報告書では、今回のような自動運転テストについてであり、歩行者が状態異常であったとしても自動運転であれば、安全方向に対応するべき
3	弱点３　歩行者の薬物摂取、飲酒等の外的要因により判断できない状況が考慮されていない	同上	何らかの薬物等の摂取について、違法か合法か以別の法律になる 国、州によって薬物の法律には違いがある 歩行者の認識が正常にできない状態であっても、誤って道路を横断している歩行者を、検出して対応できる認識能力が自動運転に必要となる 法律による一律の例外、除外は自動運転システムが危険な状態になる	報告書では、今回のような自動運転テストについてであり、歩行者が状態異常であったとしても自動運転であれば、安全方向に対応するべき
4	弱点４　自動運転では今までの運転免許だけでは十分ではない	同上	自動運転時の運転手の不注意について法整備が必要 運転中は前方を注視、回避可能な状態を維持するか、自動運転システムの認証制度により、人間の目視による判断と自動運転システムに差分がないことを条件とする 何らかの自動運転システムの認証が必要	報告書では、今回のような自動運転テストについてであり、運転手がスマホの操作など散漫な状態であっても安全方向に対応するべき 目視と同様の視認能力が必要、下記のセンサーの項目と同様
5	＜弱点1＞交通ルールの欠如（歩行者） ・以下の交通ルールに従っていなかったため車両から正しく検出されず、衝突事故にあったと考えられる。 － 交通管制信号機が作動している隣接する交差点間では、歩行者は標示された横断歩道以外の場所を渡ってはならない。 － 道を横断する歩行者は、標識のある横断歩道または交差点の標識のない横断歩道以外の場所で車道を横断する場合は、車道を走行するすべての車両に道を譲らなければならない。	事故報告に調査結果として記載済み 夜間、横断歩道のない場所で接近する車両の前を横断した歩行者の危険な行動は、アリゾナ州の法令に違反しており、薬物の使用による知覚と判断力の低下が原因である可能性がある。	歩行者に対し、交通ルールを徹底する教育が必要	車両側の対応だけではなく、歩行者に対しても注意喚起を徹底することで事故は減少すると考える。
6	＜弱点2＞メンテナンスの形骸化（歩行者）	記載なし	自転車のメンテナンスに関する仕組みづくりが必要。	自転車のライトが前方を照射していなかったことで、自動車からの発見が遅れた可能性があり、自転車のメンテナンスが不十分であったと考えられる。 自動運転の普及を考えると、ソフトウェアと合わせた対応が必要
7	＜弱点3＞注意力の欠如（運転手） ・運転手がシステムの操作の監視、運転環境の監視を怠ったことで緊急時の車両の制御ができなかったと考える。	事故報告に調査結果として記載済み 車両の運転手が注意を払っていれば、衝突を回避したり、衝撃を緩和したりするために、横断する歩行者を検知して反応するのに十分な時間があった可能性が高い。	車両の運転手が注意を払っていれば、衝突を回避したり、衝撃を緩和したりするために、横断する歩行者を検知して反応するのに十分な時間があった可能性が高い。	記載済み対象外とする
8	具体的には以下への注意が必要だった。 － ADSが解除されたことに関する通知 － 運転環境	事故報告に調査結果として記載済み Uber Advanced Technologies Groupの事故後の自動運転システムのテスト中に2人目の車両運転手を加え、運転手の注意力をリアルタイムで監視することで、事故の原因となった監督の欠陥に対処し始めた。	車両の試験の場合は、オペレータを2人以上とし、システムや運転環境の監視のみならず、ドライバーの監視を行う仕組みを組み込む	記載済み対象外とする
9	＜弱点1＞スペックの検討不足（カメラ）	記載なし	障害物を検出するカメラのスペックが低く、人間であれば検出できる対象物がカメラでは検出できていなかった可能性がある。	物体検出用に搭載するカメラ、センサーのスペックについて十分な検証を行い、基準を制定する必要がある
10	＜弱点1＞ドライバーとのコミュニケーションの欠如（HMI）	記載なし	ユーザーへの通知 ADSを解除した理由をドライバーに通知する仕組みを組み込む。 特にシステム障害により解除した場合は通知が必須。 例：解除理由をディスプレイに文字列とディスプレイの色で表示する 再設定の制限 システム障害により解除した場合は障害の原因を取り除くまでドライバーによる再設定ができなくなるような仕組みを組み込む。	ADSを解除した際に解除した理由をドライバーに通知する仕組みが必要だったと考える。
11	安全性、リスクに対する評価・冗長性への配慮不足が弱点と考えられる。	事故報告に改善事例として記載済み (1-1)衝突が発生したため、ATGは、システムがセンサー情報を融合し、可能性のある軌道を予測する方法を変更し、検出された物体が再分類されても追跡履歴を保持するようにしました(セクション1.9を参照)。(1.5.5.2)	基本的には、州の交通法に基づいた（依存した）設計がなされているが、「交通ルールを守らない対象物が路上にはある」といったことを等への配慮が全体的に不足していると考える。	対象物について「交通ルールが遵守されない」ことに対するリスク検討・安全性向上に向けた冗長的なロジック検討し追加することで事故を回避できる可能性がある。 （知覚／予測コンポーネントだけでなく、コントロール、ADS制御等のコンポーネントに対してもロジック等の追加が必要）
12	安全性、リスクに対する評価・冗長性への配慮不足が弱点と考えられる。	記載なし	車両と運転手とのインターフェースについては緊急時には運転手の判断に基づく（依存した）設計がなされているが、「運転手は不安全な運転を行う」といったこと等への配慮が全体的に不足していると考える。	緊急時には、とっさの行動が運転手にはできない可能性があることを前提とし、「緊急時に自動運転が行う最低限度の安全確保の行動」を定義することで事故の回避／衝突ダメージを低減できる可能性がある。
13	安全性、リスクに対する評価・冗長性への配慮不足が弱点と考えられる。	記載なし	車両と運転手とのインターフェースの一つに「警報」の仕組みを用いている（依存した）設計がなされているが、「運転手は警報を無視する（認識含む）／警報を切る」といったこと等への配慮が全体的に不足していると考える。	「警報」に依存した設計とする場合は、「警報無視」、「警報切」による運転手の不安全行動への対応として、自動で車両停止等による安全性確保に向けた冗長的な仕組みを検討し追加することで事故を回避できる可能性がある。
14	安全性の高い車両コントロールへの配慮不足が弱点と考えられる。	記載なし	後続車両への配慮、運転手による誤った急動作（アクセルとブレーキの踏み間違い等）への配慮により「衝突を防ぐための急制動が必要な場合には、1秒間制動を抑制するように設計された」ことで、減速されない状況で事故が発生している。	「衝突を防ぐための急制動」は運転手による依存ではなく、自動制動を実施することで回避／衝突ダメージを低減できる可能性がある。 またカメラ、センサの種別、機能、精度向上等による対応を組合わせることで、早期の検出・回避ができる可能性がある。
15	対象物に対する知覚ロジック／予測ロジックについて弱点があると考えられる。	事故報告に改善事例として記載済み (1-1)衝突が発生したため、ATGは、システムがセンサー情報を融合し、可能性のある軌道を予測する方法を変更し、検出された物体が再分類されても追跡履歴を保持するようにしました(セクション1.9を参照)。(1.5.5.2)	「知覚に関するコンポーネント」⇔「予測に関するコンポーネント」の機能連携等の配慮が不足していると考える。 【補足事項】 「対象物の分類・再分類に対する変更管理」、「対象物の分類変更があった際、それまでの履歴を利用しない仕様」等、「知覚に関するコンポーネント」⇔「予測に関するコンポーネント」の連携を指す。	「知覚に関するコンポーネント」⇔「予測に関するコンポーネント」の機能連携等の機能拡充を行うことで、事故を回避することができる可能性がある。 （知覚／予測コンポーネントだけでなく、コントロール、ADS制御等のコンポーネント間の連携に対しても機能拡充が必要）
16	対象物に対する知覚ロジック／予測ロジックについて弱点があると考えられる。	同上	「走行車線で検出された対象物」でかつ、「車両として分類された物体」について、「一般的にその車線の交通方向への走行目標が割り当てられる」設計仕様としたことで、「歩行者」、「自転車」等に知覚ロジック、予測ロジックすることへの配慮が不足していると考える。 【補足事項】 州の交通法に依存した「対象物は交通ルールを守る」ことを前提とした設計内容であったが、対象物について「交通ルールが遵守されない」ことに対するリスク検討・安全性向上に向けた冗長的なロジック検討の配慮不足。	対象物について「交通ルールが遵守されない」ことに対するリスク検討・安全性向上に向けた冗長的なロジック検討し追加することで事故を回避できる可能性がある。 （知覚／予測コンポーネントだけでなく、コントロール、ADS制御等のコンポーネントに対してもロジック等の追加が必要）
17	対象物に対する知覚ロジック／予測ロジックについて弱点があると考えられる。	記載なし	知覚ロジックにて利用するカメラ、センサの種別、機能、精度への配慮が不足していると考えられる。 （映像系のセンサに依存した設計であること） 【補足事項】 事故報告書には熱源感知センサ、音声感知センサの利用等についての記載がないため、利用されていないと考える。	今回の事故事例は車両や人通りの少ない夜の郊外道路で発生した事故であり他のセンサ類の情報を組合わせることで事故を回避できる可能性がある。
18	弱点１　現状の法律通りではあるが、現状の法律では欠点がある	事故報告に改善事例として記載済み (1-1)衝突が発生したため、ATGは、システムがセンサー情報を融合し、可能性のある軌道を予測する方法を変更し、検出された物体が再分類されても追跡履歴を保持するようにしました(セクション1.9を参照)。(1.5.5.2)	上記から引用＞ 対象物について「交通ルールが遵守されない」ことに対するリスク検討・安全性向上に向けた冗長的なロジック検討し追加することで事故を回避できる可能性がある。 （知覚／予測コンポーネントだけでなく、コントロール、ADS制御等のコンポーネントに対してもロジック等の追加が必要）	記載済み対象外とする
19	弱点２　ほかのシステムとの競合など、冗長性に問題がある	同上	上記から引用＞ 「知覚に関するコンポーネント」⇔「予測に関するコンポーネント」の機能連携等の機能拡充を行うことで、事故を回避することができる可能性がある。 （知覚／予測コンポーネントだけでなく、コントロール、ADS制御等のコンポーネント間の連携に対しても機能拡充が必要）	記載済み対象外とする
20	弱点３　インプットに対して認識システムの欠点がある	記載なし	上記から引用＞ ・知覚ロジックにて利用するカメラ、センサの種別、機能、精度への配慮が不足していると考えられる。 （映像系のセンサに依存した設計であること） 【補足事項】 事故報告書には熱源感知センサ、音声感知センサの利用等についての記載がないため、利用されていないと考える。	上記から引用＞ 今回の事故事例は車両や人通りの少ない夜の郊外道路で発生した事故であり他のセンサ類の情報を組合わせることで事故を回避できる可能性がある。
21	弱点４　システムが対応できないときに運転手に頼る必要があるが、運転手に対しての通知が遅い、効果が弱い	記載なし	安全方向に考えると自動運転にて判断できないときは、車道の端により、安全を確認して、停止することが望ましい 非安全な状態、未確定な判断で車道を走行することが非常に危険な状態を継続するため判断ができず、運転手に頼るとともに、停止を優先するべき	安全方向に対応するのであれば、自動運転にて停止を再優先するべきではないかと考える 不確定要素があれば、ドライバーに注意喚起し、反応がなければ、前後の安全を確保し、車両を停止させるなど強制的な対応も必要 レベル５であれば、他の車両にも同様の情報共有をする X地点に未確認の物体あり、確認できるまで、すべての周辺車両を停止する ⇒　電車の踏切での緊急停止ボタンのような機能
22	異常行動は制御できない			人がルールを守らないことに対する措置を行う（前提により対応が異なる） ＜守る前提＞歩行者の法律違反による事故は、車両側の過失責任なし。 ＜守らない前提＞ドライバの安全義務負荷を下げる工夫をする。 ・物理的対応（フェンス等） ・警告（電光掲示板、車内警告 等）
23	「人はルールを守る」ことが前提となっている			
24	自動化が進むほど、人の安全に対する意識はなくなる。			自動運転試験に関係ないステークホルダを巻き込む可能性のある場所での試験を禁止する。
25	自動運転に関する連邦安全基準がない。 新技術のシステムに対して、国家・政府レベルでの安全管理の監督活動や評価を行う仕組みがない。			自動運転に関する連邦安全基準を定め、国家・政府レベルでの安全管理の監督活動を行う。 もしくは、新技術というリスクが不透明な事業に対しては、安全基準やリスク評価を具体的に検討するための体制を構築することをプロセスとして定める。
26	企業として安全文化・方針の浸透、安全管理業務・安全リスクマネジメントを行う組織がなく、安全管理者の任務が確実に行われていることが確認できない			企業としての安全管理業務および安全リスクマネジメントを行う専任組織を設置し、安全管理と安全リスクマネジメントの確実な実施を図るとともに、安全管理が確実に実施されていることを確認する
27	運用開始時、または定期的に、従業員に対して遵守すべき重要事項の確認行為を行っていない			遵守すべき重要事項は、適切なタイミング（就事時、または定期）で検査・監査を行い遵守状況を確認する。
28	循環・定期的等タイミングを設けて、遵守状況の監査を行っていない			
29	自動運転時の不遵守状況が適切に監視されていない			
30	州から企業に対する規制が不十分			州として ・企業に対して、安全性の監督と規制を行う体制、仕組みを構築し適用させる ・体制や仕組みを構築する以前に不透明な場合でも、州としてリスク評価を行う体制を構築する。
31	自動運転の安全性に関する方針は示しているが、関係者が行うべき安全性自己評価プロセスが不十分。 安全基準の策定、性能評価の試験手順の提示が具体的でなく、具体的な実施基準・評価の仕組みとして示されていない。			適所レベルで安全性自己評価プロセスと実施基準を定め、行うべき対象者に実施を義務付ける
32	国及び地方自治体の既存も代表する団体であり、管理、法執行、モデルプログラム開発を開発。高速道路の安全問題のための情報交換所としての役割を果たしているが、新しい技術が出る文脈では関わりが不透明。 他の州からの情報を踏まえて法整備プロセスに関与していない、州への規制不十分			適所のすべての州が事業者に対して、新技術を含む安全対策に対する規制が図れるよう、各州との情報連携を行い、安全管理の法やモデルプログラムを浸透させる。そのための体制を構築する。

付録14_CAST分析の作業工数等参考データ

（単位：h）

	付録名	Aさん	Bさん	Cさん	Dさん	Eさん	合計
CAST1,2	付録2	25	8	2	2	2	39
CAST3	付録4、付録5	10	2	4	3	3	22
CAST4	付録2	15	7	5	3	5	35
CAST5	付録3	5	4	5	3	4	21
CAST6	付録6	5	2	4.5	4	4	19.5
CAST7.8	付録7	5	2	4	4	4	19
CAST9	付録8	5	3	1	4	2	15
	合計	70	28	25.5	23	24	170.5

＜補足情報＞

（1）CAST分析は，5名で行った．

その内訳は，分析に要した時間は171時間（1人あたり34時間），導出した問題点は32件（内18件 は想定外の新たな問題点）．「導出した問題点1件」に対する「分析に要した時間」は１件当たり5.3時間（=171時間／32件），1人あたりユニークで6件導出（=32件／5人）することができた．

自動運転関連の専門家ではない我々によるリスク導出作業ではあるが，分析に掛かるコストは比較的低コストで実施できたと考える．

（2） 参考文献[A]では，概要および事例が掲載されており分析初心者でも概要理解がしやすいため，当初はそれに従って分析を試みた．

しかし，各Stepに対する成果物が分析を進める上で不明瞭であり，各Stepの反復作業が多く，チームでの分担作業には向かないと考えた．

そのため過去事例のある参考文献[B]の手順に切り替えた．

これにより成果物が明確になり，分担作業ができ，手順ベースによる作業状況の確認・意見のすり合わせができた．

＜参考文献[A]＞

Nancy G. Leveson， CAST HANDBOOK: How to Learn More from Incidents and Accidents, 2019

＜参考文献[B]＞

日科技連ソフトウェア品質管理（SQiP）研究会第35年度演習コースⅢ，
CASTとFRAMによるセキュリティ事故分析～システム思考とレジリエンス～，2020.2