

## 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）  
 里富 豊（リコー IT ソリューションズ）  
 研究員：鎌田 桂太郎（アイホン）  
 黒田 知佳（テックエンジニアリングソリューションズ）  
 松崎 美保（TIS）  
 西 啓行（富士通）  
 大森 裕介（エフ ソルアヴァシス）  
 主 査：金子 朋子（国立情報学研究所）  
 副 主 査：高橋 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<sup>[1]</sup>．

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<sup>[2]</sup>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<sup>[3]</sup>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うことで、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。

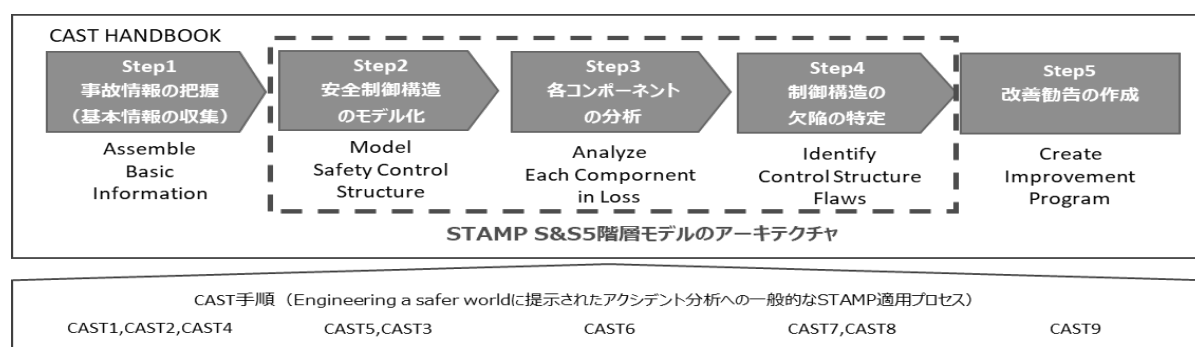


図 1： CAST 分析のステップ

- (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<sup>[10]</sup>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?:原因究明の為に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<sup>[10]</sup>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<sup>[10]</sup>を参照）。

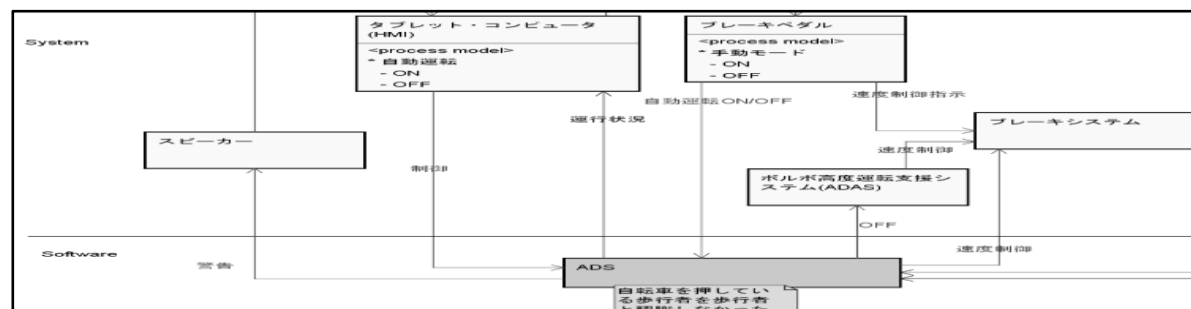


図 2：安全 CS

### 【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<sup>[10]</sup>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<br>(抽象的事象) | CAST6-1        | CAST6-2                 | CAST6-3                      | CAST6-4                    |
|----------|---------------------|----------------|-------------------------|------------------------------|----------------------------|
|          |                     | 安全上の責務<br>(責任) | 非安全なCA                  | プロセス/メンタル<br>モデルの欠陥          | 意思決定された<br>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<sup>[10]</sup>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       |           |                  | CAST8         |
|--------------------|---------|---------|-------------|---------|--------|----------|-------------|-----------|------------------|---------------|
|                    |         |         |             |         |        |          | 安全リスク評価・冗長性 | 設計不備・考慮漏れ | 安全なマネジメントシステムの設計 | 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<sup>[10]</sup>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<sup>[10]</sup>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<sup>[10]</sup>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<sup>[10]</sup>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・予測不備による事故・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による事故・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による事故・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<br>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      |
|                                   | 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               |
| 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    | 対応漏れが出ないような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 |
|                                   | 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<br>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                                                   | 異臭に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<br>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。                                     | 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                                                     |
|                                   | 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<sup>[10]</sup>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。

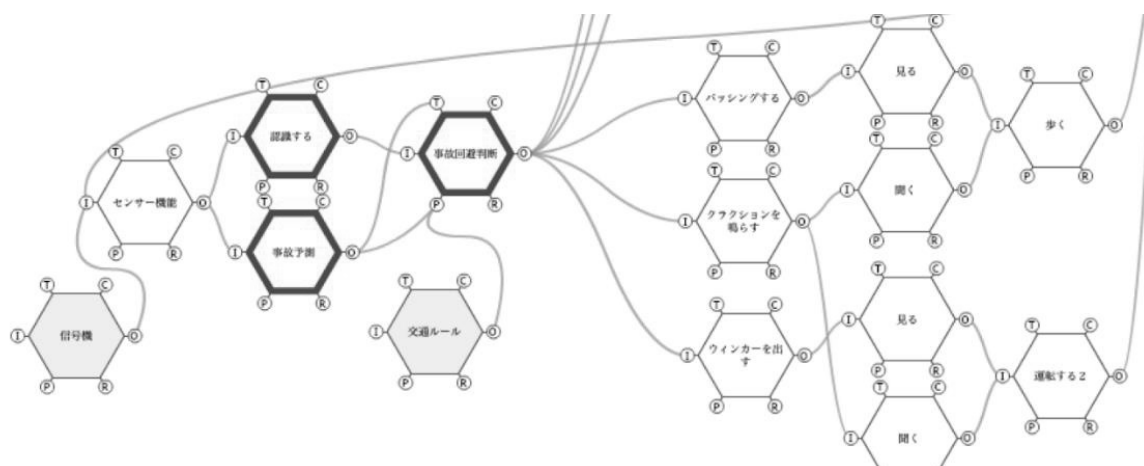


図 3：FRAM モデル

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づきを得る事ができ、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を示すことができるのではないかとと思われる。

### 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。

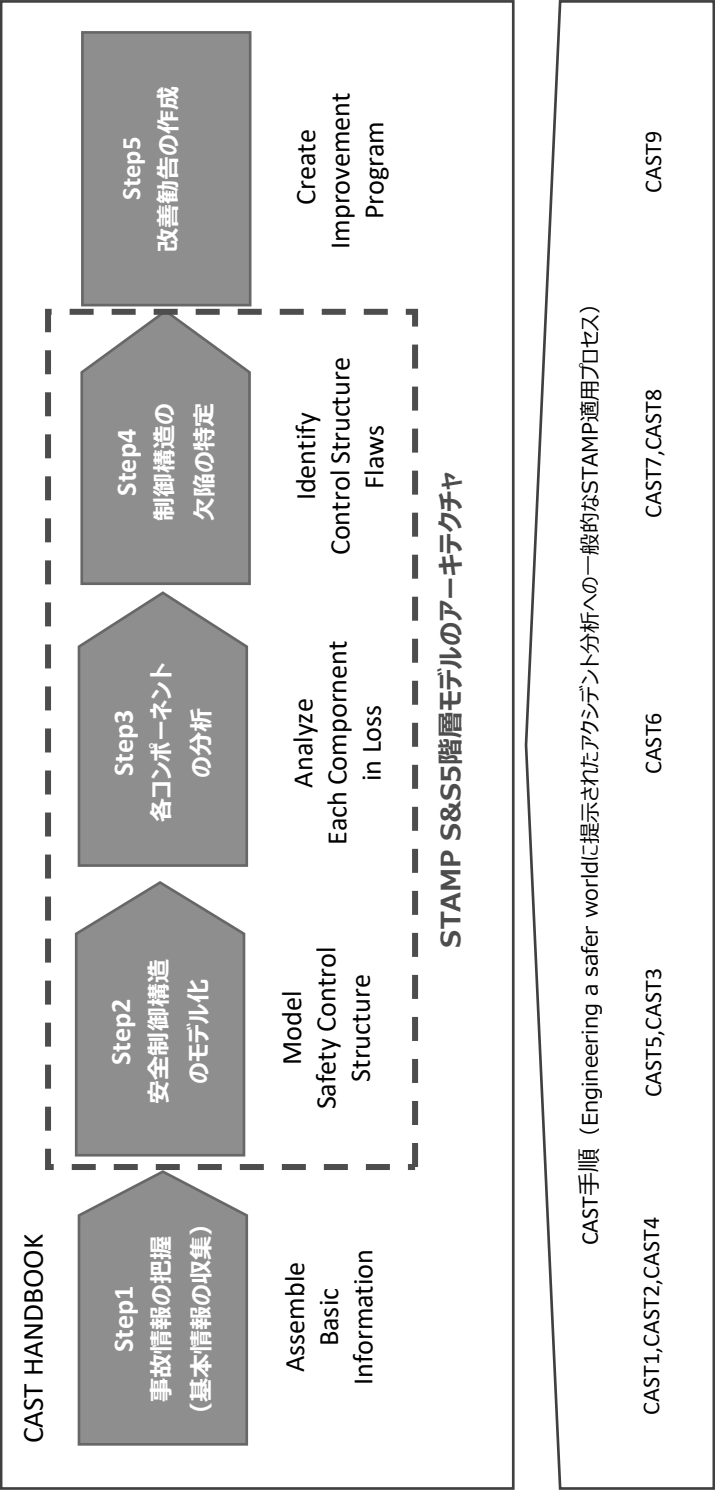
## 参考文献

- [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](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



- 
- <sup>1</sup> 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](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
- <sup>2</sup> 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
- <sup>3</sup> 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
- <sup>4</sup> 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
- <sup>5</sup> Nancy G. Leveson, Engineering a Safer World, MIT Press, 2012
- <sup>6</sup> 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
- <sup>7</sup> Hollnagel. E, 社会技術システムの安全分析—FRAM ガイドブック, 2013
- <sup>8</sup> 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
- <sup>9</sup> Nancy G. Leveson, CAST HANDBOOK: How to Learn More from Incidents and Accidents, 2019
- <sup>10</sup> 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

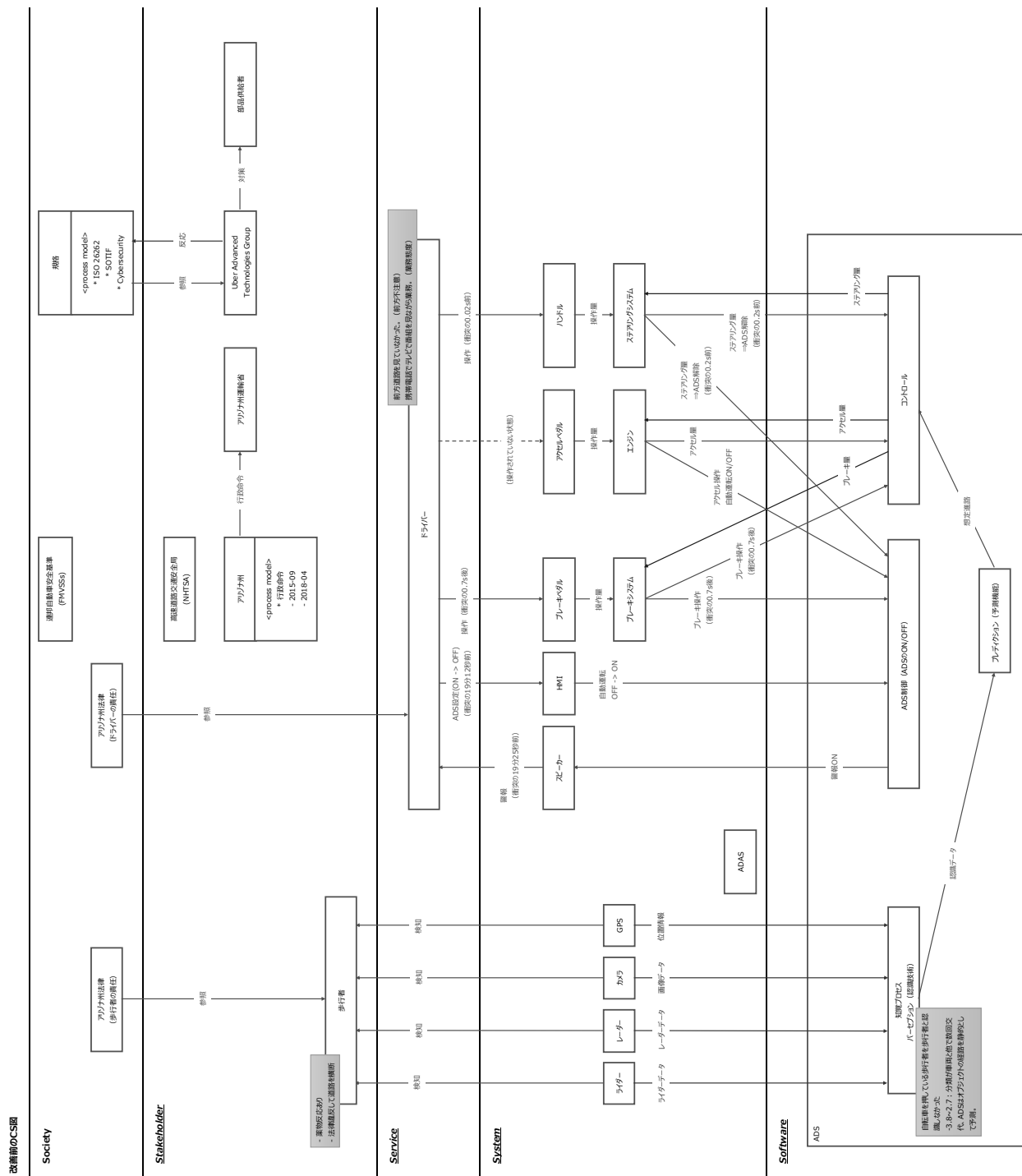
付録1\_図1：CAST分析のステップ



[illegible]

付録3\_表2：具体的コンポーネントレベルでの分析結果

[illegible]





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        | 高位レベルの事象<br>(抽象的事象)    | CAST6-1<br>安全上の責務(責任)                                                            | CAST6-2<br>不完全なソフトウェアアクション<br>(CS部品の責任をイメージ)                                                      | CAST6-3<br>プロセス/メンタルモデルの欠陥                                                                                                                                                                                                                             | CAST6-4<br>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送ること。                                                           | ――                                                                                                | ――                                                                                                                                                                                                                                                     | ――                                                                                                                                                                                                               |
| 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                                                                      | (1-1)・対象（歩行者）を正しく判断できない条件があった<br><br>カメラの映像について正確に知覚プロセスに送ることについては警告音に記載がないため割り下げられないことより、こまめとした。 | (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。<br><br>(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)<br><br>(1-3) 走行車線や横断線、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力への歩行者の割り当てがなされる。(1.5.3.2)<br>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)・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。<br>(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   |             |                        |                                                                                  |                                                                                                   |                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                  |
| A12   |             |                        |                                                                                  |                                                                                                   |                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                  |
| A13   | System      | カメラ、センサ                | ・捉えた映像を正確に知覚プロセスに送ること。<br>(運転手が見ていた状況と同じ情報が取得できること)                              | 映像の状況、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)<br><br>(1-1)運転手が見ていたものを正確に描写できなかった                   | ――                                                                                                                                                                                                                                                     | ・新しく販売された自動車は、前部、後部、およびペダルに反射器を有し、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た。<br><br>・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？<br><br>・自転車のライトが地面に直視に照らされ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<br><br>(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)(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。                                                                                                                                                                                                            | ――                                                                                                                                                                                                               |
| 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<br><br>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)              | (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)                                                                                                                                                                                                             | ――                                                                                                                                                                                                               |
| A24-2 |             |                        | 軌跡を継続的に更新する(1.5.5.2)                                                             | (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<br><br>(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。<br><br>(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。<br>(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<br><br>(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。<br><br>(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。<br><br>現在検出されている位置は静的なものとなされ、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)                                                                           | (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できなかった<br><br>(1-2)・信号無視の歩行者を歩行者として認識しなかった<br><br>・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)                                                         | (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)横断が発生したため、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更新し、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)<br><br>(1-1)システムが検出した歩行者の位置を確認して代替経路を計算する<br>(1-2)車両の運転者や車両を制御する際、ADS が制御を制御する 1 秒間であった。(1.5.5.3) |
| 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)・危険な状況を検出した後、衝突を避けるために 0.71g 以上の急制動が必要な場合には、1秒間制動を抑制するようにADSを設計していた(2.2.1.1)                                                                                                                                                                      | (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更新し、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)<br><br>(1-1)システムが検出した歩行者の位置を確認して代替経路を計算する<br>(1-2)車両の運転者や車両を制御する際、ADS が制御を制御する 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)オペレータが長時間車道から離れて世界を見ていた<br>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れ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、車両の制動を車両運転者に頼っていた(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                                                                 | 実際の歩行者検知(1.5.4.2)<br>・行動制動が始まる。(1-2)                                                              | (1-2)<br>- 自転車の周りを保護するためのADSワーキングプラン(0.3秒前に生成)ができなかった<br>- 状況が危険(緊急事態)になる。<br>歩行者との衝突が起っていると判断し、緊急事態を検知しました。<br>- 行動制動が始まる。                                                                                                                            | (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動を取り、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)オペレータが長時間車道から離れて世界を見ていた<br>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れ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、車両の制動を車両運転者に頼っていた(2.2)                                                                                                                                           |
| B4    | Software    | コントロール                 | 車両制動（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)                                     | 車両制動の真実検出時に、運転者の操作が必要(1.5.7.30項に記載)。<br>(1.4.5.3 オペレータプロトコル)                                      | 真実検出時に運転者への警告(1)への配慮不足(1.4.3 オペレータ訓練)                                                                                                                                                                                                                  | 運転者は、ハンドルの上の手を置いて、ブレーキペダルの上足を乗せる前提の設計(1.4.3 オペレータ訓練)                                                                                                                                                             |
| B6    | Software    | コントロール                 | 衝突を感知がある場合、車両を減速もしくは停止させる                                                        | 行動制動の実施に伴い十分に減速できない、もしくは減速できない<br>・緊急時の対応は通常の運転手だった                                               | ・システムの認識を緊急時に、行動制動を実施する設計。<br>・緊急時の対応は通常の運転手だった                                                                                                                                                                                                        | 最大歩行制動(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、車両の歩行を開始する設計)                                                                                                                                                                  |
| 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際、ADS が制動を抑制（1 秒間）する設計(1.5.5.3)                                                                                                                                                                                                             | 安全の冗余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緊急警告を鳴らす。                                                             | 急ブレーキが必要な時に運転手に警告を鳴らしていない<br>(1.5.6.1.1)                                                          | システムは事前にADSが歩行者中であることを運転者に警告したが、運転者に鳴らされた。                                                                                                                                                                                                             | 運転者と車両間の(1)の/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、運転者に緊急警告を鳴らす<br>。(1.5.6.1)                                             | 緊急ブレーキの必要時、緊急警告が鳴っていない。(1.5.6.1)                                                                  | 徐々に減速を開始しながら、運転者に緊急警告を送る設計(1.5.5.3)                                                                                                                                                                                                                    | 自動による急制動時、緊急ブレーキ時、急激な動きの変化なしに滑らかに減速を維持するよう、車両制動する設計(1.5.5.3)                                                                                                                                                     |
| B12   | System      | ADS制御                  | 歩行者の検出に、運転者に緊急警告を送る。(1.5.4.2)                                                    | ドライバーが歩行者の位置を認識し、ADSを再設計した。(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。                                                                                                                                                                          |
| B13   | System      | ADS制御                  | 車両制動時に制動が開始を知らせる。(1.5.5.3)                                                       | 車両制動時、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)                                                                                                                                                                                                                             | 制動の態を考慮した(1.5.5.3)                                                                                                                                                                                               |
| B15   | System      | ADS制御                  | (1.6)<br>・前方衝突が起っていることをドライバーに警告する (FCW)<br>・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)ADSを無効にしていた                                                                                  | (1-1)レーダーの制動に関する検証ができていない<br><br>(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<br><br>(1-3)ADSを併用しようとした場合、開閉に時間がかかると考えられていた？                                                                                                                                          | (1-1)ゴールがATGシステムのレーダーが同じ周波数で動作するため、制動動作と考えていた<br><br>(1-2)ゴールがAEBとATGの両方からブレーキコマンドを受信した場合、正しく動作しなかった。                                                                                                            |
| 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した経路はその目的に依存していた。(1.5.5.2)                                                                                                                                                                                                          | ――                                                                                                                                                                                                               |
| C1    | 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                                                                          | 歩行者が横断を見て守る前提となっている                                                                                                                                                                                                                                    | 人は法律を守る                                                                                                                                                                                                          |
| C2    | 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                                                                          | 歩行者が横断を見て守る前提となっている                                                                                                                                                                                                                                    | 人は法律を守る                                                                                                                                                                                                          |
| C4    | 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いない前提となっている                                                                                                                                                                                                                                  | 車道内からフンス等を設けるのは不可能？<br>歩きづらくすればいいと思った？                                                                                                                                                                           |
| C5    |             |                        |                                                                                  |                                                                                                   |                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                  |
| C6    | Stakeholder | 歩行者                    | 法律を守る                                                                            | 歩行者が法律に違反する                                                                                       | 真実者の行動を前提にしている                                                                                                                                                                                                                                         |                                                                                                                                                                                                                  |
| C7    | Society     | 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（自動車技術者協会）ATG（先進技術グループUber）がドライバーに警告する仕組みを準備しない                               | ・真実者の行動を前提にしている<br>・歩行者が横断を見て守る前提となっている<br>・歩行者が車道に入っていない前提となっている<br>・ドライバーが正しく運転する前提となっている                                                                                                                                                            | ？                                                                                                                                                                                                                |
| C8    | Stakeholder | ATG                    | ・安全文化、方針を定める<br>・安全管理が行われていることを確認する<br>・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<br>安全リスクマネジメントが行われていない                                                  | 安全管理体制がない<br>企業の安全文化・方針浸透を確認しない                                                                                                                                                                                                                        |                                                                                                                                                                                                                  |
| C9    | Stakeholder | ATG                    | 安全方針の遵守と監視                                                                       | 従業員が遵守する歩行者管理業務の運用を行っていない                                                                         | 制約遵守確認の欠陥                                                                                                                                                                                                                                              |                                                                                                                                                                                                                  |
| C10   | Stakeholder | ATG                    | 安全方針の遵守と監視                                                                       | 従業員が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                    | 車両制動と監視                                                                          | 従業員が車両制動の監視を行っていない                                                                                | 運転者の真実検知とフィードバックが不十分                                                                                                                                                                                                                                   |                                                                                                                                                                                                                  |
| C12   | Stakeholder | ATG                    | 歩行者の検出と監視                                                                        | 従業員が歩行者の検出と監視を行っていない                                                                              | 制約遵守確認の欠陥                                                                                                                                                                                                                                              |                                                                                                                                                                                                                  |
| C13   | Society     | ADOT                   | 州としての企業に対する安全監督・規制                                                               | 自動運転の試験を行う企業に対する規制行為の対象（リスクに対応して）課税されていない                                                         | 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<br>・自動運転車に対する安全基準を策定する<br>・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<br>安全性自己評価プロセスが不十分<br>・安全基準の策定<br>・歩行者の検出と監視業務の提示<br>が最低限ではない                           | 方針は示しているものの、対象者が具体的に対応するような行動指針・遵守レベルが不明確かつ指示されていない                                                                                                                                                                                                    |                                                                                                                                                                                                                  |
| 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規制に関与する                            | 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規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されていない？(各州間の連携も含め)                                                                                                                                                                                                               |                                                                                                                                                                                                                  |
| 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 | ドライバー                  | 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義務を怠らしていない                                                                                                                                                                                                                               | 自動運転への適性                                                                                                                                                                                                         |
| C18   | Stakeholder | ドライバー                  | ドライバーは運転に集中しない                                                                   | 運転に集中していない                                                                                        | 自動運転車両とドライバーの義務が曖昧になっている。                                                                                                                                                                                                                              | 自動運転への適性                                                                                                                                                                                                         |

付録7\_表4：システムの俯瞰分析結果

[illegible]



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

| 例  | 特徴                        | 分析から見える弱点                                                                                                                                                                                                                                         | 改善動向案                                                                                                                                                          |
|----|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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先になる                                                                                                                                                                                                            | 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<br>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<br>自動運転時の運転者の状態を管理、監視する機能の具体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高い                                                                                                                                                                                                                          | 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<br>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<br>横断を禁止するのであれば、標をつけるなど、物理的な対策が必要<br>何らかの異常等の原因について、適法か違法かは別の法律になる |
| 3  |                           | 歩行者の乗物接触、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                                                                                                                                                                                                             | 国、州によって乗物の法律には違いがある<br>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なもの<br>法律による一律の例外、例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視について法整備が必要<br>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がないことを条件とする                                                           |
| 5  |                           | 自動運転に関する連邦安全基準がない                                                                                                                                                                                                                                 | 何らかの自動運転システムの認証が必要<br>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                                                                                                 |
| 6  | 人に関するもの                   | 交通ルールの文知（歩行者）<br>以下の交通ルールに従っていなかったため車両から近く検出されます。衝突事故にあったと考えられます。<br>→ 交通規制（信号機）が作動している関係する交通機関では、歩行者は提示された横断歩道以外の場所を渡ってはならない。<br>→ 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横断を横断する場合は、車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  |                           | メンテナンスの形態化（歩行者）<br>自転車ライトが前方を照射してなかったことで、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）<br>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。<br>→ ADSが解除されたことに関する通知<br>→ 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、衝突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つた可能性が高い。<br>車内の試験の場合は、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）<br>→ 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。<br>→ 守らない前提＞ドライバーの安全義務を負わせる工夫をする。                                                      |
| 10 |                           | 「人はルールを守る」ことが前提となっている                                                                                                                                                                                                                             | → 物理的対応（フェンス等）<br>→ 警告（電光掲示板、車内警告 等）                                                                                                                           |
| 11 |                           | 自動車が走むほど、人の安全に対する意識はなくなる。                                                                                                                                                                                                                         | 自動運転試験に際してはステークホルダを巻き込み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                | → スペックの検出不足（カメラ）<br>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。                                                                                                                                                                     | 物体検出に際してはカメラ、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 |                           | → 警報に関する検出不足<br>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<br>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。<br>特にシステム障害により解除した場合は通知が必須。<br>例：解除理由をディスプレイに文字列とディスプレイの赤で表示する                                                      |
| 14 |                           | → ドライバーとのコミュニケーションの欠如（HMI）<br>ADSを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<br>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<br>→ 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える。                                                                                                                                | 対象物について「交通ルールが遵守されない」と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。<br>（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の安全確保の行動」を定義することで事故の回避／被害ダメージを軽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（誤検知）／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える。                                                                                                                                         | 「警報」に依存した設計とする場合は、「警報無視」、「警報切り」による運転手の不安な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 |                           | → 急制動への対応について（安全性の高い車両コントロールへの配慮不足）<br>→ 後続車両への配慮、運転手による誤った急制動（アクセルとブレーキの踏み間違ひ等）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」とことで、回避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／被害ダメージを軽減できる可能性がある。<br>またカメラ、センサーの検知、機能、精度向上等による対応を組み合わせることで、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<br>→ 「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える。<br>【補足事項】<br>「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」の連携を調べる。                                             | 「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。<br>（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）                             |
| 20 |                           | → 「走行車線や検出された対象物」でかつ、「車両として分類された物体」について、「一般的にその車両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える。<br>【補足事項】<br>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」と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」と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。<br>（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 |                           | → 知覚ロジックに利用するカメラ、センサーの検知、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）<br>【補足事項】<br>事故報告書には動体検知センサ、静止画検知センサの制限等についての記載がないため、利用されていないと考ええる。                                                                                                         | 今回の事故事例は車両や人通りの少ない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み合わせることで事故を回避できる可能性がある。                                                                                             |
| 22 | 企業安全文化・マネジメントシステムに関するもの   | 企業としての安全文化、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実行さ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動を行っていない                                                                                                                                                                                                        | 遵守すべき重要事項は、適切なタイミング（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） | 臨時・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                                                                                                                                                                                                                   |                                                                                                                                                                |
| 25 |                           | 自動運転時の不遵守状況が適切に監視されていない                                                                                                                                                                                                                           |                                                                                                                                                                |
| 26 |                           | 州から企業に対する規制が不十分                                                                                                                                                                                                                                   | 州として<br>→ 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<br>→ 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                                                                   |
| 27 |                           | 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                                                                                                                                                                                                     | 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                                                                                                                     |
| 28 |                           | 安全基準の策定、性能評価の試験手続の提示が具体的になく、具体的な実施基準、評価の仕組みとして定まれている                                                                                                                                                                                              |                                                                                                                                                                |
| 29 |                           | 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、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、州への規制不十分                                                                                                               | 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。                                                                         |

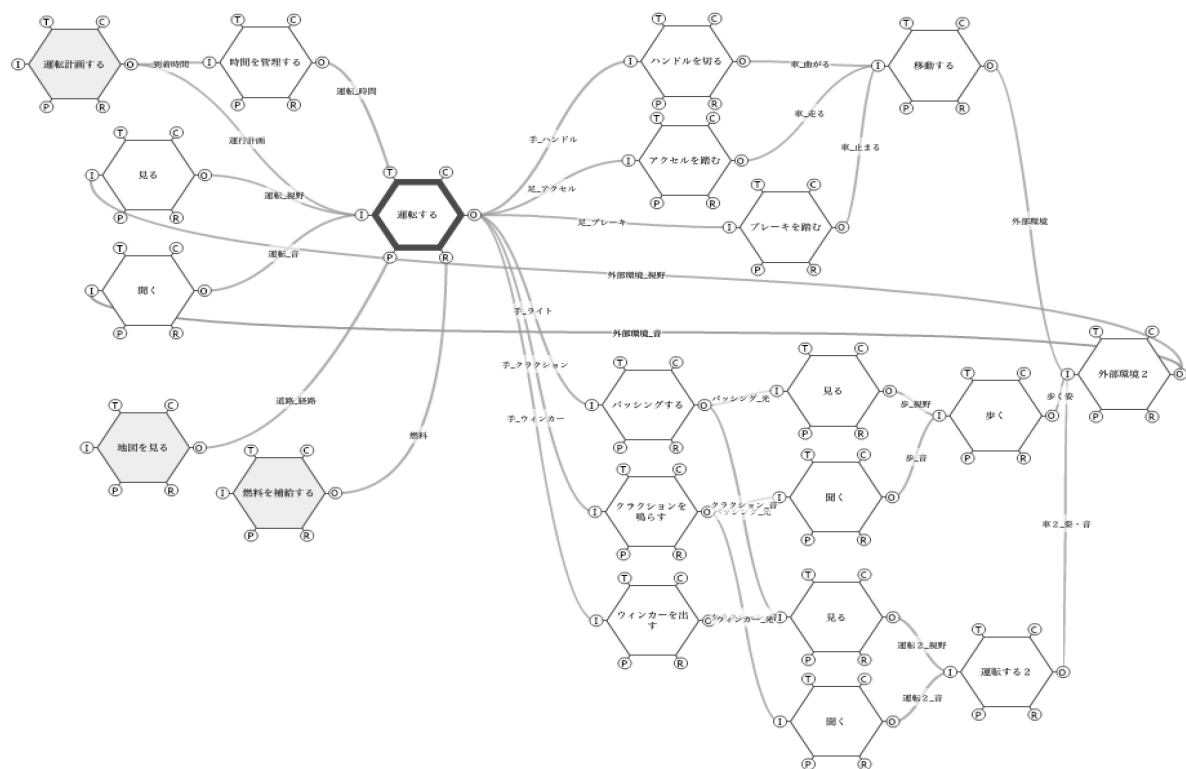
付録9\_表6：コンポーネント抽出表

| 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・ジャイロセンサー）           | 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<br>駐車支援のアラウンドモニターを計測<br>車線維持を目的とした白線認識<br>交通標識の認識<br>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)<br>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)<br>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)<br>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)<br>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)<br>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)<br>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）                      | 異臭による異常を感知                                                                            | 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）)<br>判断 (To: 運転者（聴覚）)<br>判断 (To: 運転者（嗅覚）)<br>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）                     | 異臭による異常を感知                                                                            | 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)                                                                |         |     |             |

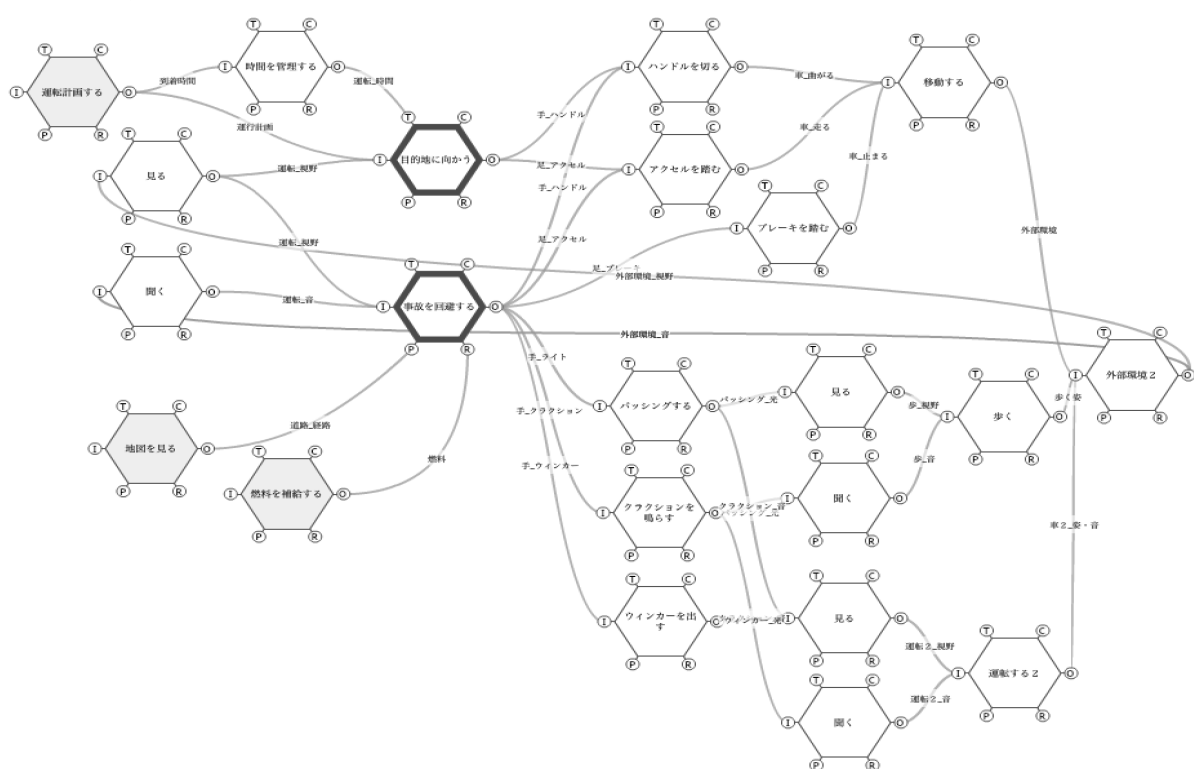
付録10\_表7：対策表

| HCFlD       | 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は衝突の5.6秒前に歩行者を検出。<br>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<br>[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告を鳴らした。                                                                                                                            | M2   | Uber ADSでは警告を鳴らし始めたが運転手は間に合わなかった。<br>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<br>[SC22]                                                                    |             |                                                                                           |
| HCf2-N-1-1  | 今回のケースでは、通行人は自動車を確認することが出来ていなかった                                                                                                                                                        | M3   | 今回のケースでは、乗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。<br>そのような人物である場合は、道路に入場させない。<br>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<br>[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。<br>通常ならクラクションやバッシングでの注意喚起を自動で行うことも対応可能と思われる。 |
| 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、乗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。<br>そのような人物である場合は、道路に入場させない。<br>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) 自動車を運ぶる認識で、車両・身体の損失または人命の損失<br>[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。<br>通常ならクラクションやバッシングでの注意喚起を自動で行うことも対応可能と思われる。 |
| HCf22-T-1-1 | ブレーキによる遅すぎる減速は発生した。（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では警告を鳴らし始めたが運転手は間に合わなかった。<br>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) ブレーキによる不意な不停止・停止により事故につながる<br>[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では警告を鳴らし始めたが運転手は間に合わなかった。<br>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<br>[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・予測不備による事故・違反が起きる<br>[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による事故・違反が起きる<br>[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<br>[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による事故・違反が起きる<br>[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<br>[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ならず事故につながる<br>[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<br>[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  | 対応遅れが出ないよう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<br>保安基準を満たせず責任を問われる<br>[SC26] |             |                                                                                           |
| HCf4-N-1-1  | 自動運転レベル3 報告書ではバッシングの自動機能なし                                                                                                                                                              | M11  | レベル3では、バ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・他自動車へバッシングによる注意が伝わらず事故につながる<br>[SC17]                                                                |             |                                                                                           |
| HCf4-T-1-1  | 自動運転レベル3 報告書ではバッシングの自動機能なし                                                                                                                                                              | M11  | レベル3では、バ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) 遅すぎるバ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<br>[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、減速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<br>[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) 臭臭による故障に気付かない<br>[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<br>走行の安定感がない<br>[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検討の考慮が必要                                                                                                                               | (UCA44-N-1) 交通ルールを侵害し罪に問われる<br>[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の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<br>[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。<br>システムが差し追った衝突を検出した場合、ドライバーに警告するが、自動的にブレーキをかけます。<br>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<br>[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。<br>Uber ADSでも人という認識はされていないが「ADSは衝突の5.6秒前に歩行者を検出」している。ボルボADASの「前方衝突警告」でも、衝突の2.5秒前に移動するため、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<br>[SC22]                                                                    |             |                                                                                           |
| HCf10-N-1-1 | 警察が視認性を確認したところ、街灯が歩行者の道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<br>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<br>[SC3]                                                       |             |                                                                                           |
| HCf44-N-1-2 | 米高速道路交通安全局(NHTSA)は、FOW、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。<br>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<br>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。<br>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<br>[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<br>[SC25]                                                              |             |                                                                                           |

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～

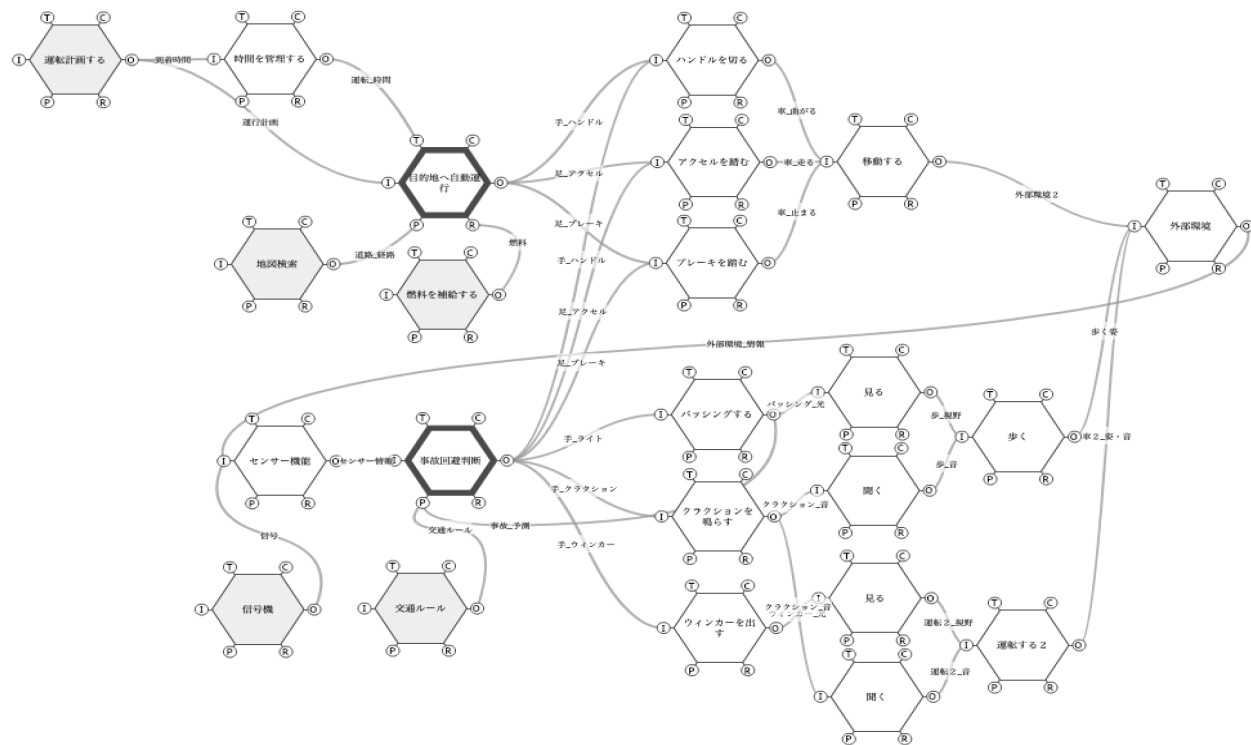


自動運転レベル0（人間が運転する場合）のFRAM図 ～「運転する」機能を「目的地に向かう」「事故を回避する」機能に分解～

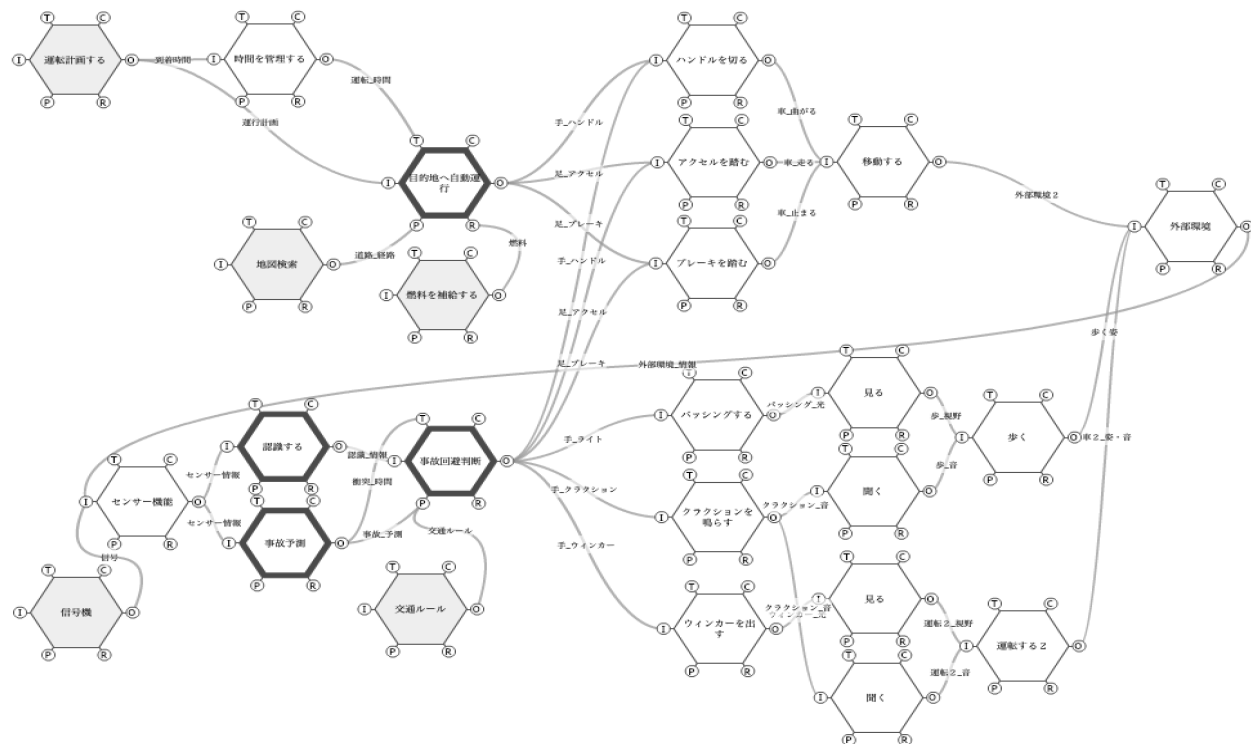


付録12\_図3：FRAMモデル（2/2）

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）

[illegible]

## 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