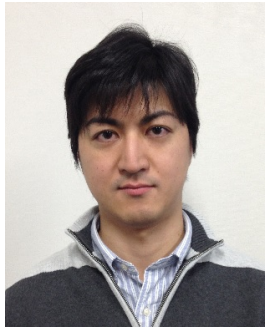
Safety Engineering for Automotive ML-controlled System

2019年11月7日 MaaS DIY Day@北海道大学

SEAMS & TIGARS プロジェクト

松原 豊（Yutaka MATSUBARA）
名古屋大学 大学院情報学研究科 准教授
E-mail : yutaka@ertl.jp
Web : https://www.ertl.jp/~yutaka

自己紹介



本務

- 名古屋大学 大学院情報学研究科
  情報システム学専攻 高田・松原研究室 准教授
  未来社会創造機構 モビリティ社会研究所 准教授
  附属 組込みシステム研究センター 協力教員

その他主な役職

- 自動車技術会 共同研究センター 自動運転に係わる総合信頼性の継続的確保に向けた標準化検討委員会 幹事
- NPO法人 TOPPERS プロジェクト運営委員
- (一社)ディペンダビリティ技術推進協会 自動車応用部会 主査
- 電子情報通信学会情報セキュリティ 情報セキュリティ 研究専門委員
- セキュリティキャンプ全国大会 講師
- 技術アドバイザ（組込み関係企業）

主な産学連携研究プロジェクト

- University of York, Assuring Autonomy International Programme, 「Towards Identifying and closing Gaps in Assurance of Autonomous Road Vehicles (TIGARS)」研究メンバ
- 平成29年度戦略的基盤技術高化支援事業「自律的自動運転の実現を支える人工知能搭載システムの安全性立証技術の研究開発」(SEAMSプロジェクト)サブリーダ

CASE from Daimler AG at CES 2017

Connected（つながる）

- つながるクルマは運転者を支援し，さらに周辺と通信する

Autonomous（自律的な）

- 自律的な乗りもので，スムーズな交通流，柔軟な計画，ストレスフリーな移動

Shared & **S**ervices（共有 & サービス）

- 自分のクルマやその他の交通手段によって，素早く柔軟に目的地に到達

Electric（電動化）

- 電動化された乗りものとサービスインフラが未来を作る

https://www.daimler.com/documents/investors/reports/annual-report/daimler/daimler-ir-annual-report-2017.pdf を参考に独自に日本語訳を作成

自動運転（Autonomous）・共有（Shared/Services）に関連する実証実験

自動運転サービスの開発・運用における課題

対象システムの大規模化と変化への対応

- 開発段階ですべての要求を満たすよう努力がなされるが，大規模化，複雑化によって困難な場合も
- 運用段階における変化への対応も想定

サービス中心のビジネスモデルへの変化

- 個々の組込みシステム（機器）の開発から，人間，クラウド，環境などと連携・連動するサービスへ
- SoS（System of Systems）によるサービス提供

非機能要件に対する重要性の維持・高まり

- 利用者が求める信頼性，安全性やセキュリティ等の非機能（ディペンダビリティ）要件の重要性は不変
- 一方で，開発，運用では低コスト化も要求される

自動運転サービスの開発効率の維持・向上と
ディペンダビリティをどう両立するか？

自動運転システムの安全性に関する基本的な指針

国連での議論

Safety Vision の抜粋

automated vehicle systems, under their operational domain (OD), shall not cause any traffic accidents resulting in injury or death that are reasonably foreseeable and preventable

Framework document on automated/autonomous vehicles, WP.29-177-19, Mar. 2019

国土交通省の安全ガイドライン

自動運転車の運行設計領域(ODD) において、自動運転システムが引き起こす人身事故であって合理的に予見される防止可能な事故が生じないこと

国土交通省自動車局，自動運転車の安全技術ガイドライン，平成30年9月

自動運転システムから安全と安心へ

短期的な対応　　**車両レベルの安全性の議論**

- 運転中（サービス中）に発生する問題に即時的に対応し，事故を防止する
- 例：故障，誤使用，性能限界等への対応

長期的・継続的な対応

- 運転中に発生した問題の原因を追求し改善
  - 例：要求仕様の変更/追加，ソフトウェア更新，セキュリティ対策
- サービスの維持，継続と説明責任
  - 例：サービス内容の更新，事故情報の公開等

車両レベルだけでなく，サービスレベルの安全性と
サービス継続性（レジリエンス性）が十分であることを説明
（納得・信頼してもらうための説明＝アシュアランス）

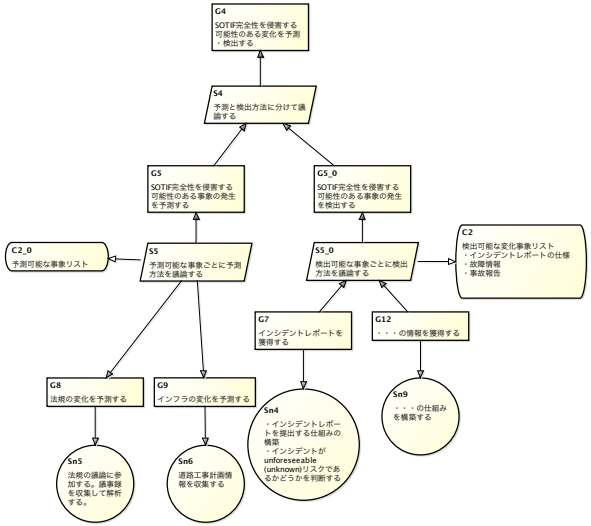
安全性論証手法の共同研究プロジェクト

1. 自律的自動運転の実現を支える人工知能搭載システムの安全性立証技術の研究開発（サポイン）
   - Witz，アーク・システムソリューションズ，名大, アイシン精機, ヤマハ など
   - 2017-2019年度 → **SEAMSプロジェクト**として継続
2. Towards Identifying and closing Gaps in Assurance of Autonomous Road Vehicles (**TIGARSプロジェクト**)
   - Adelard Ltd., City University of London, 名大, 神奈川大学, Witz
   - 2018年9月-2019年12月

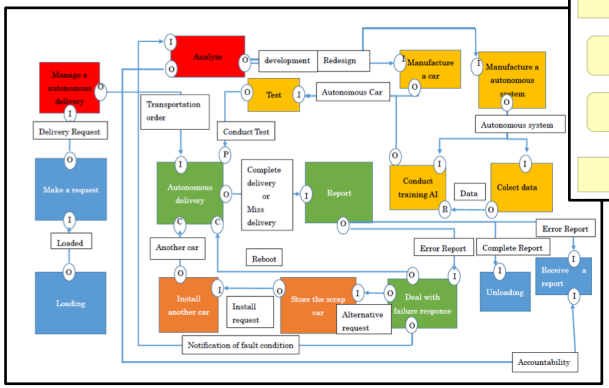
機械学習（AI）を使用したコンポーネントを搭載する車載制御システムの安全性論証方法，テスト手法，安全対策（例えば，誤認識の検出）を検討

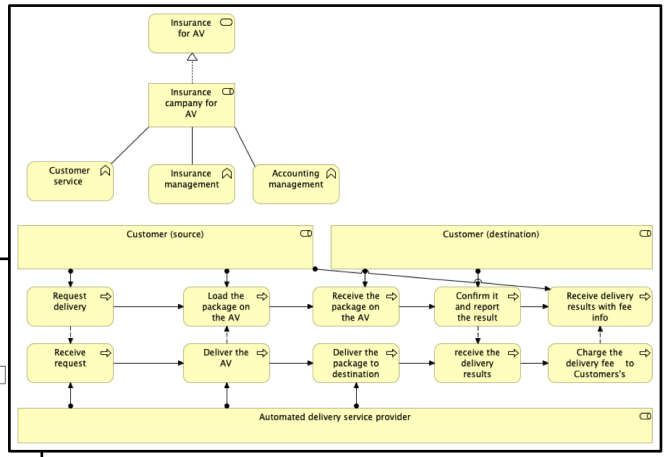
安全性論証手法の共同研究プロジェクト

安全性論証フレームワーク

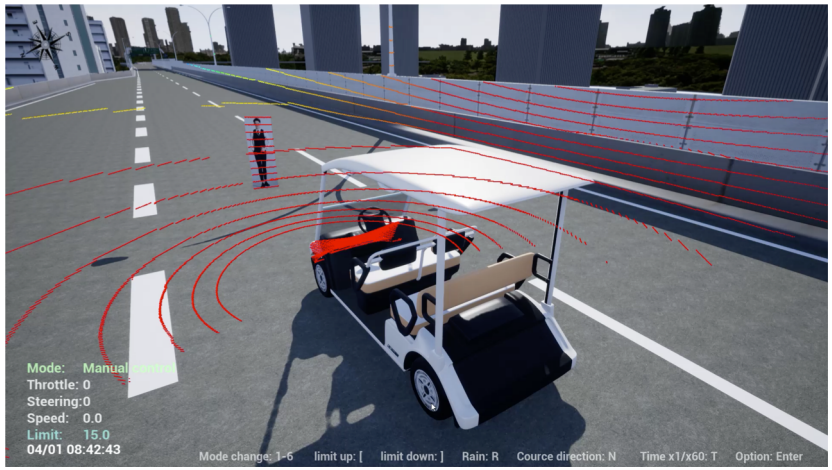


モデル化，分析手法





シミュレーションによるテスト



実機環境

継続的な安全性論証フレームワーク

モビリティサービスの安心と社会受容性の醸成に向けた分析と論証技術

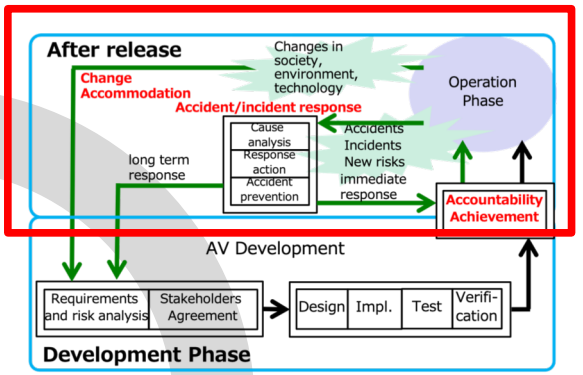
車両だけでなく，サービス全体での説明と論証を支援する仕組みの提案

(1) モビリティサービスのモデリング手法の開発
(2) サービス運用を含めたライフサイクルの規定
(3) サービスレベルでの安全性とレジリエンス性の分析手法の開発

→ 日本発の国際規格IEC 62853を活用

参照

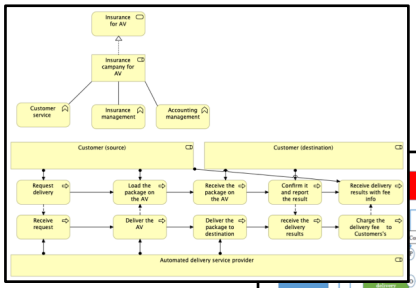
(2)モビリティシステムのライフサイクル



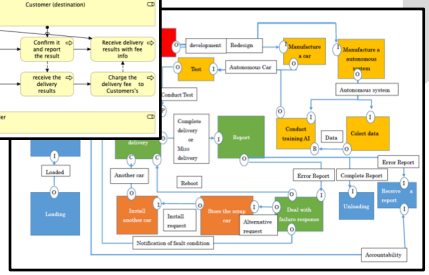
サービス運用時のリスク管理，社会や環境の変化への対応を重視

安全に関する国際規格議論に提案中

(1)モビリティサービス(MaaS)のモデリング



ArchiMate

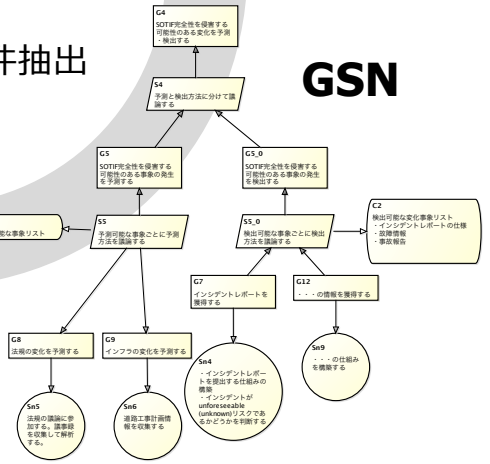


FRAM

車両だけでなく，販売者，利用者，保守者等の全ステークホルダを明確化

要件抽出

(3)安全性とレジリエンス性分析



GSN

サービスの安全性や緊急時対応等の説明に役立つ論証フレームワーク

既存サービスの検証や改善にも活用可能

まとめ

- 車両レベルでの安全性の議論，国際規格化が活発
- 安心や社会受容性を維持・向上するにはサービスレベルでの議論が必要
- SEAMプロジェクトとTIGARSプロジェクトでは，AI搭載車両の安全性の論証と対策技術を研究・開発
- TIGARSプロジェクトでは，さらに，IEC 62853をベースとした自動運転サービスのディペンダビリティ論証フレームワークを提案
- ライフサイクル全体に渡って継続的にチェック，改善をすすめることが重要
- 今後の計画
  - ビジネス視点でのモデル化を推進（ArchiMate）
  - 運用段階の要件を国際規格の議論の場に提案
  - 実サービスへの適用

参加・協力メンバを募集中！