自動運転車の安全性を数学的に証明するには？

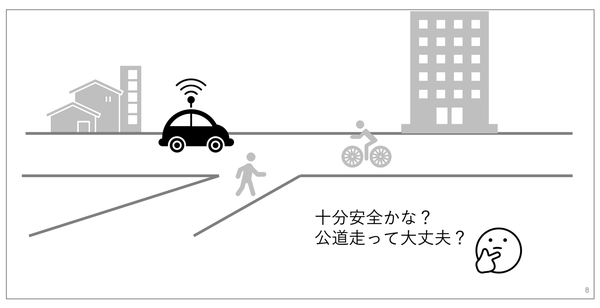
プログラム論理による 自動運転安全性の形式検証

～ ICT新技術の社会受容のための数学と論理学 ～

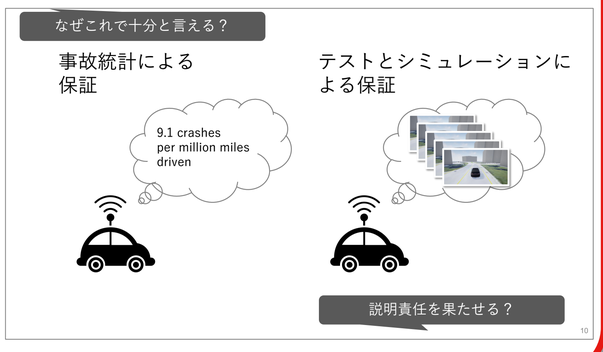
蓮尾 一郎, Clovis Eberhart, James Haydon, Benjamin Bray, 諏訪 敬之 他
数理的高信頼ソフトウェアシステム研究センター／ERATO 蓮尾メタ数理システムデザインプロジェクト

自動運転の本格普及を妨げる 安全性保証の課題

- 自動運転の普及には 非常に高い安全性が必要
- **ただ安全なだけではダメ**. 説明して，納得してもらい，社会に受け入れてもらう必要がある



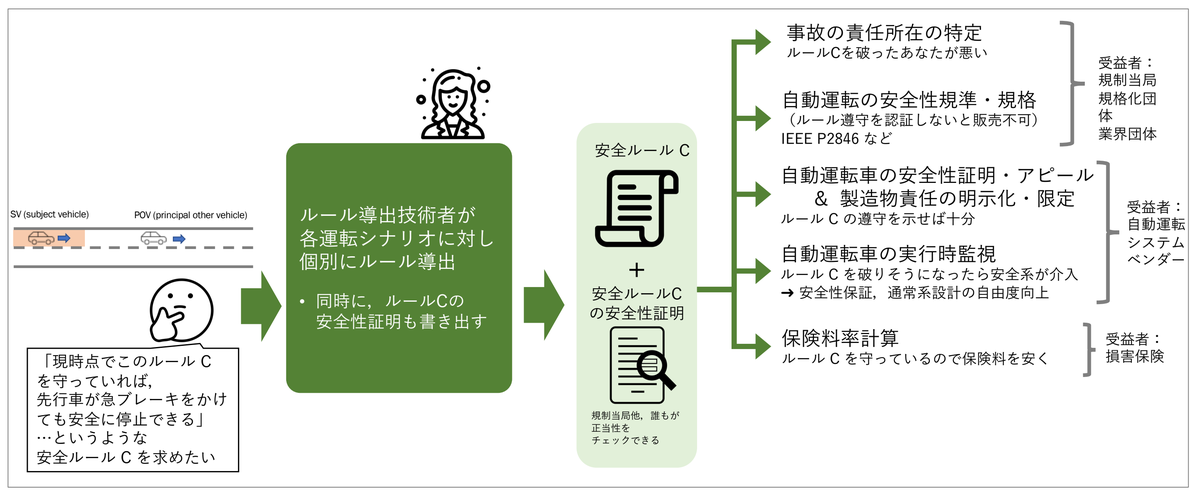
- 現在の主流は統計的安全性保証（事故統計，テスト）. しかし，保証の強さや説明可能性などの問題がつきまとう



ライブデモ実施中！

安全性証明済みの自動運転車に イジワルしてみよう！
事故を起こすことができるかな？

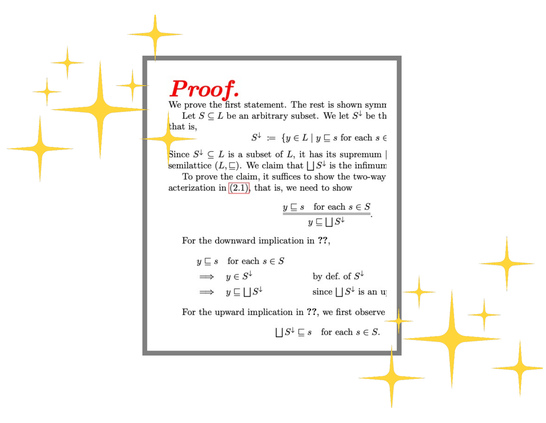
社会応用： 自動運転エコシステムの あらゆる場面でインパクト



- 安全規格，交通法規，製造物責任の基準など，**社会的契約**としての安全ルール（数学的証明というお墨付きあり）
- 自動運転の普及の現状（安全性の基準が定まらない，製造物責任の上限が見えず事業展開ができない）を打破

成果概要： 自動運転の安全性を 数学的に証明する技術

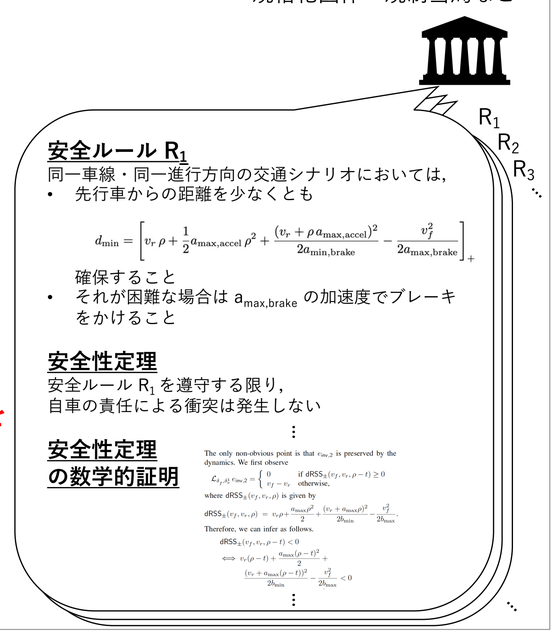
- 決して事故が起こらないことを **数学の定理として厳密に証明**
- 保証度合いの**絶対の強さ**（数学的証明に例外はない）
- 高い**説明可能性**（証明のステップを追いかけていけば安全性の論理的説明になる）



具体的成果： 安全性証明付きの 安全ルールを提供

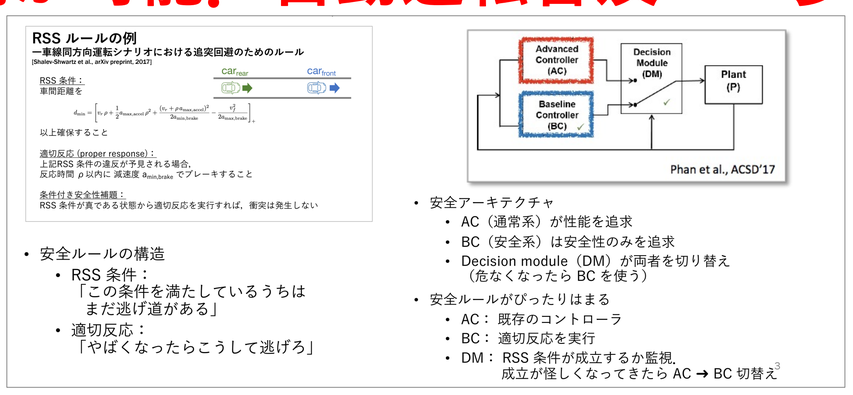
RSS 技術概要
[Shalev-Shwartz et al., arXiv, 2017]
[Hasuo, Eberhart, Haydon, ⋯, Kamijo, Shinya, Suetomi, IEEE T-IV, in press]

規格化団体・規制当局など



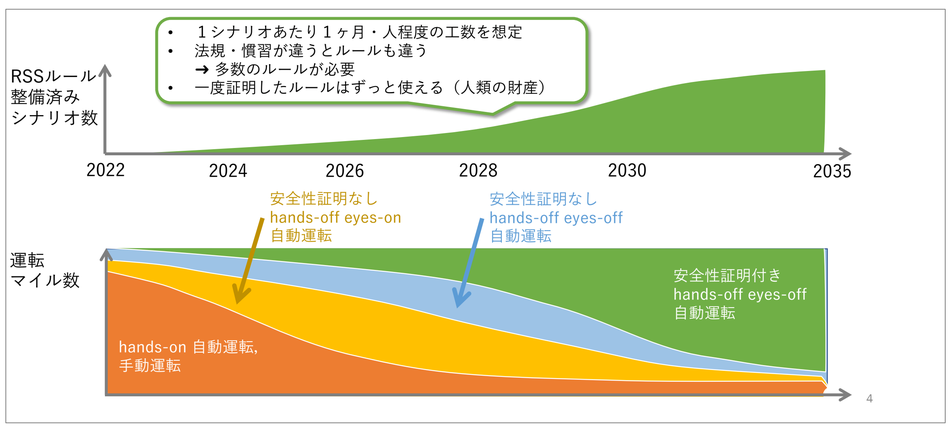
- **「自動運転安全性の数学的証明」という夢を論理的安全ルールという現実として実現**
- 安全ルールは汎用 ➔ 規準・規格として社会受容を促進
- 方法論を Mobileye/Intel が提唱 [Shalev-Shwartz et al., arXiv, 2017] ➔ 実用に不可欠な論理的技術を我々が開発（マツダ株式会社との共同研究）

成果展開： 現実を見据えた漸進的 展開が可能．自動運転普及へ一歩一歩



- 安全ルールの構造
  - RSS 条件：「この条件を満たしているうちはまだ逃げ道がある」
  - 適切反応：「やばくなったらこうして逃げろ」
- 安全アーキテクチャ
  - AC（通常系）が性能を追求
  - BC（安全系）は安全性のみを追求
  - Decision module（DM）が両者を切り替え（危なくなったら BC を使う）
- 安全ルールがぴったりはまる
  - AC： 既存のコントローラ
  - BC： 適切反応を実行
  - DM： RSS 条件が成立するか監視，成立が怪しくなってきたら AC ➔ BC 切替え

- （数学的証明付き）安全ルールは，**既存の自動運転システムにレトロフィットできる**．安全系・冗長系として



- ルールセットの完成を待たず**今すぐ実応用できる技術**. 安全ルールを増やしていくことで ODD を漸進的拡大

連絡先：国立情報学研究所 数理的高信頼ソフトウェアシステム研究センター長 蓮尾 一郎
URL： https://group-mmm.org/eratommsd/ Email： hasuolab-secr@nii.ac.jp