



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 ～

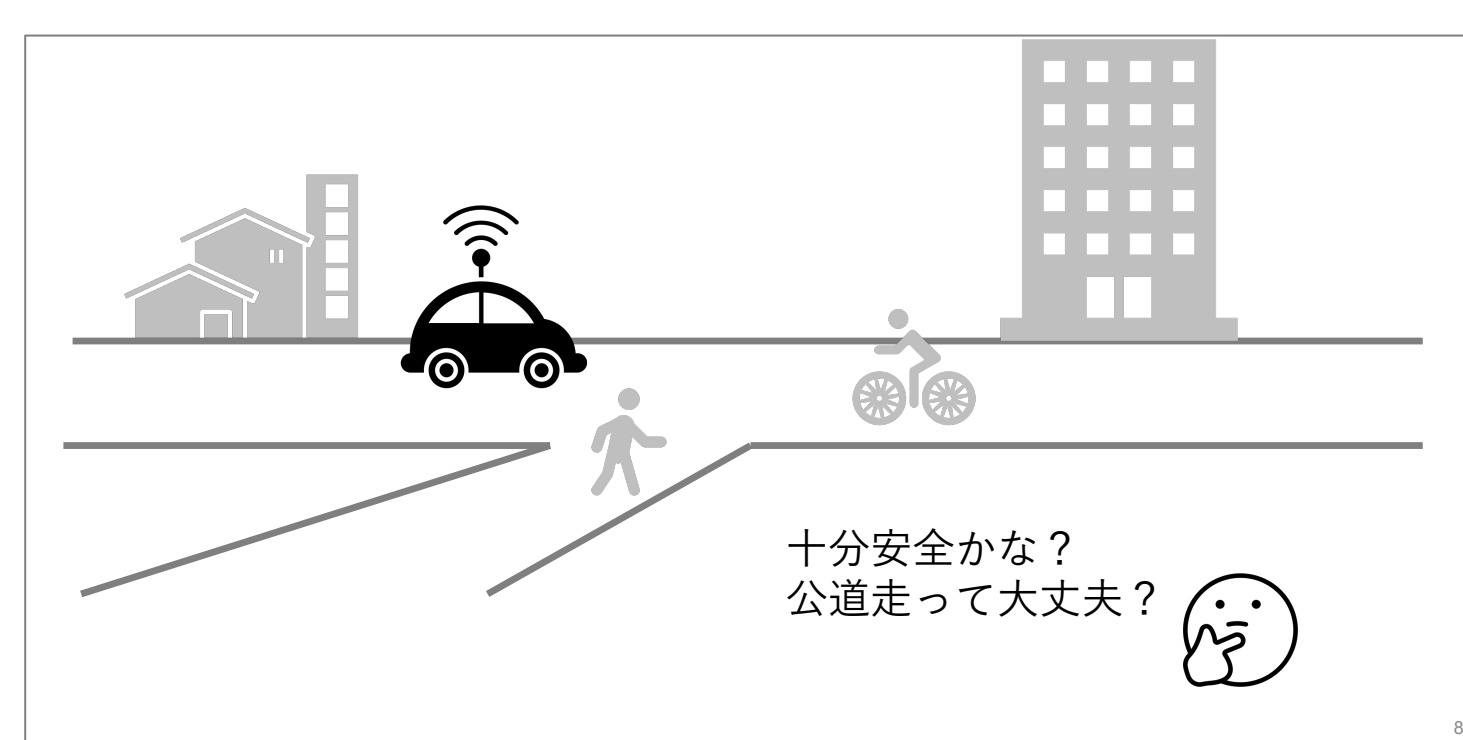


蓮尾 一郎, Clovis Eberhart, James Haydon, Benjamin Bray, 諏訪 敬之 他

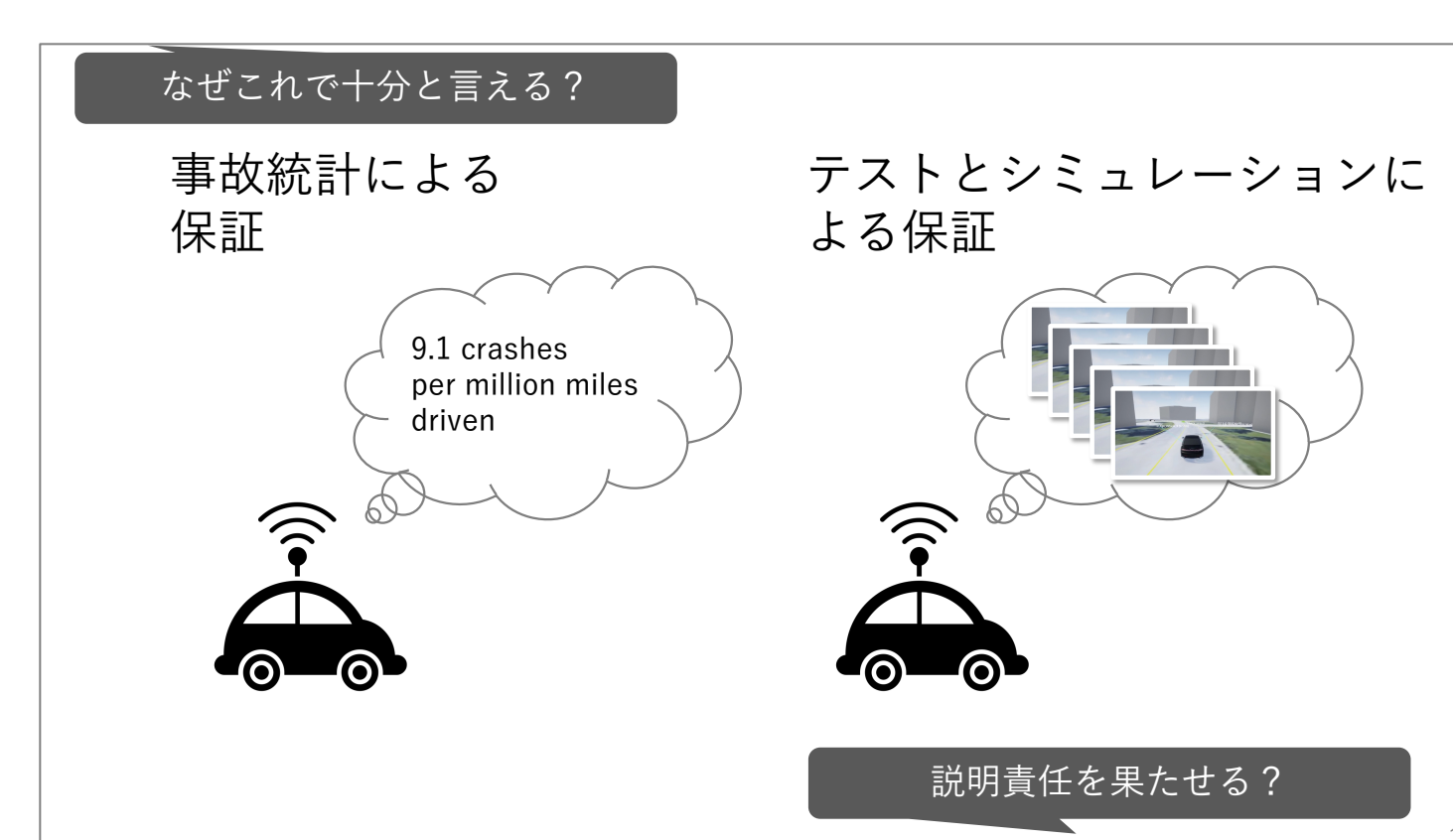
数理的高信頼ソフトウェアシステム研究センター／ERATO 蓮尾メタ数理システムデザインプロジェクト

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

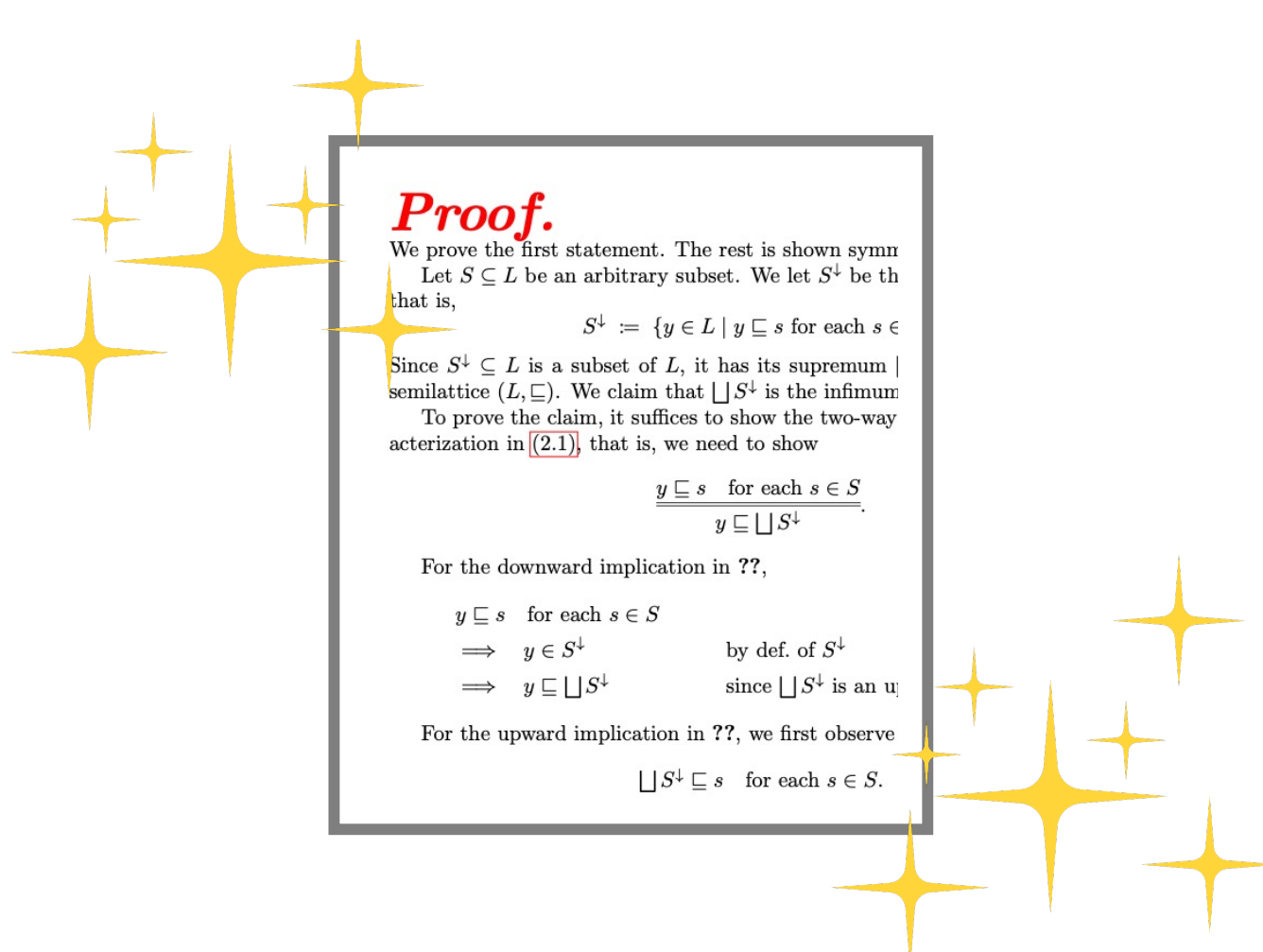


- 現在の主流は統計的安全性保証（事故統計，テスト）。しかし，保証の強さや説明可能性などの問題がつきまとう



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]

「安全ルール R₁, R₂, ... を遵守します。よって安全」

「安全ルール R₁, R₂, ... を遵守します。よって安全」

「安全ルール R₁, R₂, ... を遵守します。よって安全」

- 「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）

規格化団体・規制当局など

安全ルール R₁
同一車線・同一進行方向の交通シナリオにおいては、
・ 先行車からの距離を少なくとも

$$d_{\min} = \left[v_r \rho + \frac{1}{2} a_{\max, \text{accel}} \rho^2 + \frac{(v_r + \rho a_{\max, \text{accel}})^2}{2 a_{\min, \text{brake}}} - \frac{v_r^2}{2 a_{\min, \text{brake}}} \right]_+$$

確保すること
・ それが困難な場合は a_{max,brake} の加速度でブレーキをかけること

安全性定理
安全ルール R₁ を遵守する限り、
自車の責任による衝突は発生しない

安全性定理の数学的証明

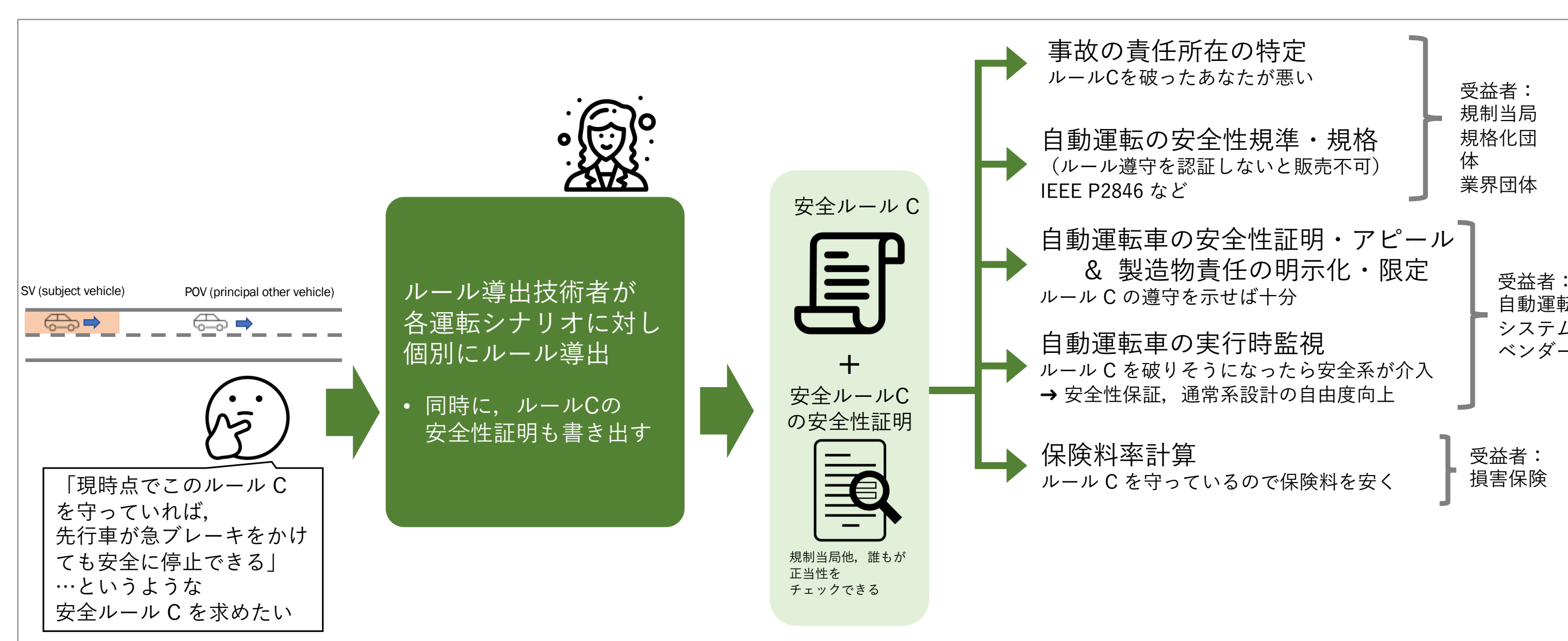
The only non-obvious point is that v_{max} is preserved by the dynamics. We first observe
C₁(t) v_{max} = 1 if v_r = v_{max}, otherwise,
since dBS₁(t, v_r, ρ) is given by
dBS₁(t, v_r, ρ) = v_r ρ + 1/2 a_{max, accel} ρ² + (v_r + ρ a_{max, accel})² / (2 a_{min, brake}) - v_r² / (2 a_{min, brake})
Therefore, we can infer as follows,
dBS₁(t, v_r, ρ) < 0
⇔ v_r ρ + 1/2 a_{max, accel} ρ² + (v_r + ρ a_{max, accel})² / (2 a_{min, brake}) - v_r² / (2 a_{min, brake}) < 0
⇔ (v_r + ρ a_{max, accel})² / (2 a_{min, brake}) < v_r² / (2 a_{min, brake}) - v_r ρ - 1/2 a_{max, accel} ρ²

- 「このルールを守れば絶対に安全（と証明済み）」という**数学的安全ルール**を提供
- いわば **数学的道路交通法**
- Shalev-Shwartz らの方法論を，論理学（プログラム論理）によって形式化・拡張。
適用範囲を大きく拡大 [Hasuo, Eberhart, Haydon, et al. IEEE Trans. Intell. Vehicles, 2022]

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。自動運転普及へ一步一步

RSS ルールの例
→ 直線前方交通シナリオにおける追突回避のためのルール
[Shalev-Shwartz et al., arXiv preprint, 2017]

RSS 条件：
安全ルールを遵守すること
以上を確保すること

適切反応 (proper response)：
上記RSS 条件の違反が予想される場合、
反応時間 ρ 以内で 減速度 a_{max,brake} でブレーキすること
条件付き安全状態確保
RSS 条件が真である状態から適切反応を実行すれば、衝突は発生しない

- 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)
- 安全ルールがびったりはまる
・ 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³

- （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

RSSルール整備済みシナリオ数

2022 2024 2026 2028 2030 2035

安全性証明なし hands-off eyes-on 自動運転

安全性証明なし hands-off eyes-off 自動運転

安全性証明付き hands-off eyes-off 自動運転

運転マイル数

hands-on 自動運転, 手動運転

- 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