Behaviour Specifications of Autonomous Vehicles

Nok Wongpiromsarn

October 3, 2019

Contributions by
A. Censi, K. Slutsky, J. Fu, E. Frazzoli

Formal methods provides a proof that a system satisfies its specification

	Closed system synthesis / traditional model checking	Probabilistic synthesis	Reactive synthesis	Minimum violation planning
System	Deterministic	Probabilistic	Nondeterministic (adversarial)	Deterministic
Guarantee on the policy	Satisfy the spec	Maximize the probability of satisfying the spec	Satisfy the spec for all possible adversarial actions	Minimize the violation of the spec
Computational nature	Offline / online	Offline	Offline	Online, anytime
Rely on	Satisfiability of the spec	An accurate probabilistic model of the environment	An accurate assumption of the environment behaviors and realizability of the spec	Real-time planning to respond to quickly changing environment
Applications	Analysis of Toyota unintended acceleration, mission critical software (Mars Science Laboratory, Deep Space 1, Cassini, the Mars Exploration Rovers, Deep Impact, etc.)	Case studies in communication, network and multimedia protocols, security and biology	Case studies in robot motion planning	Decision making component of some autonomous vehicles

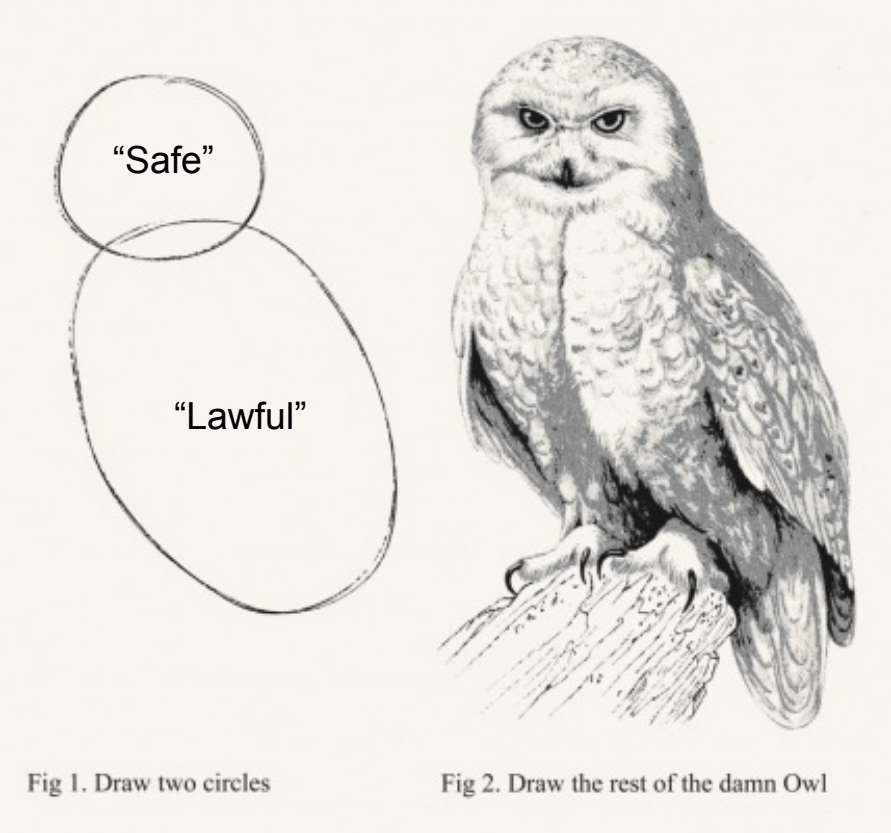
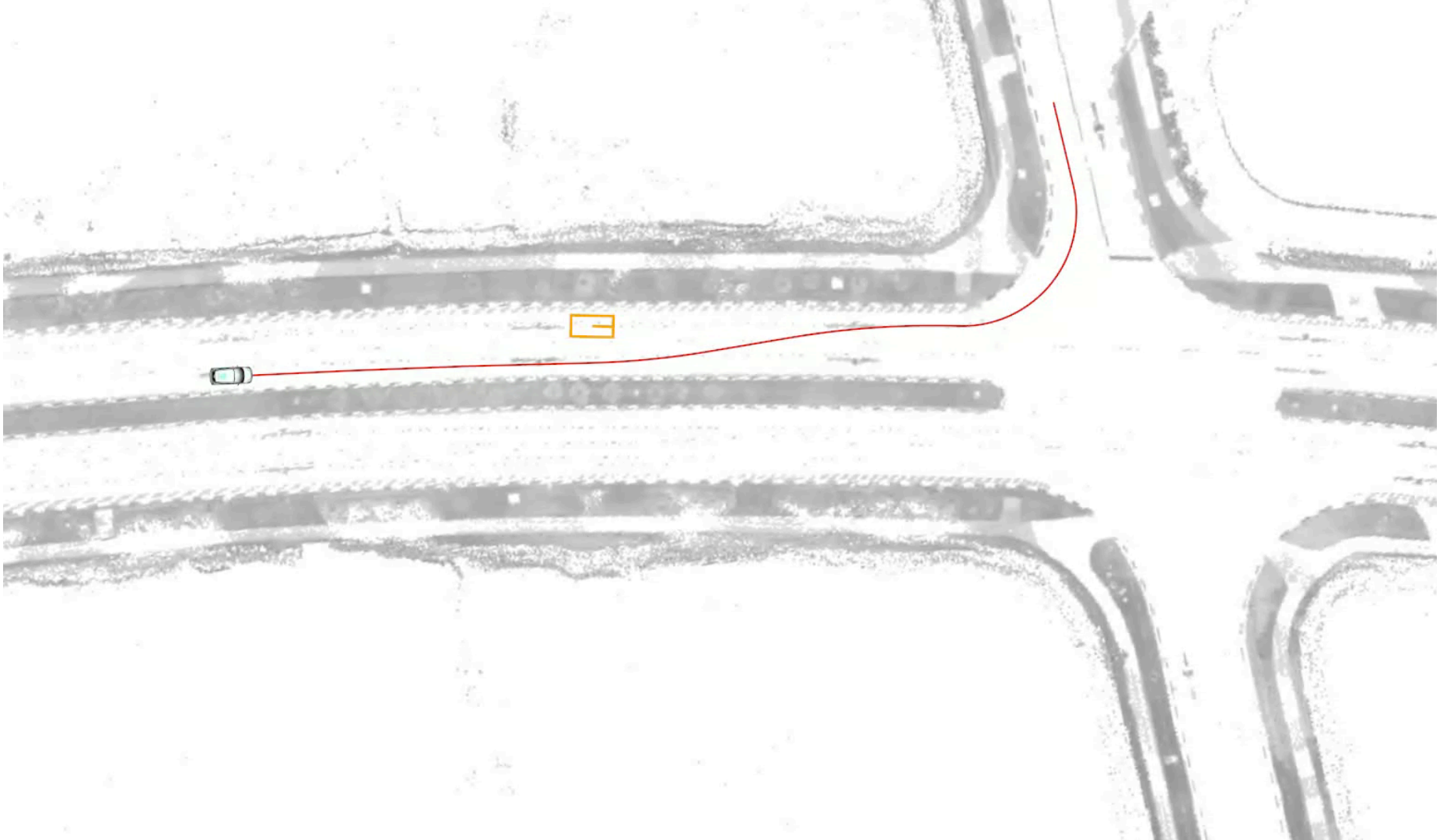


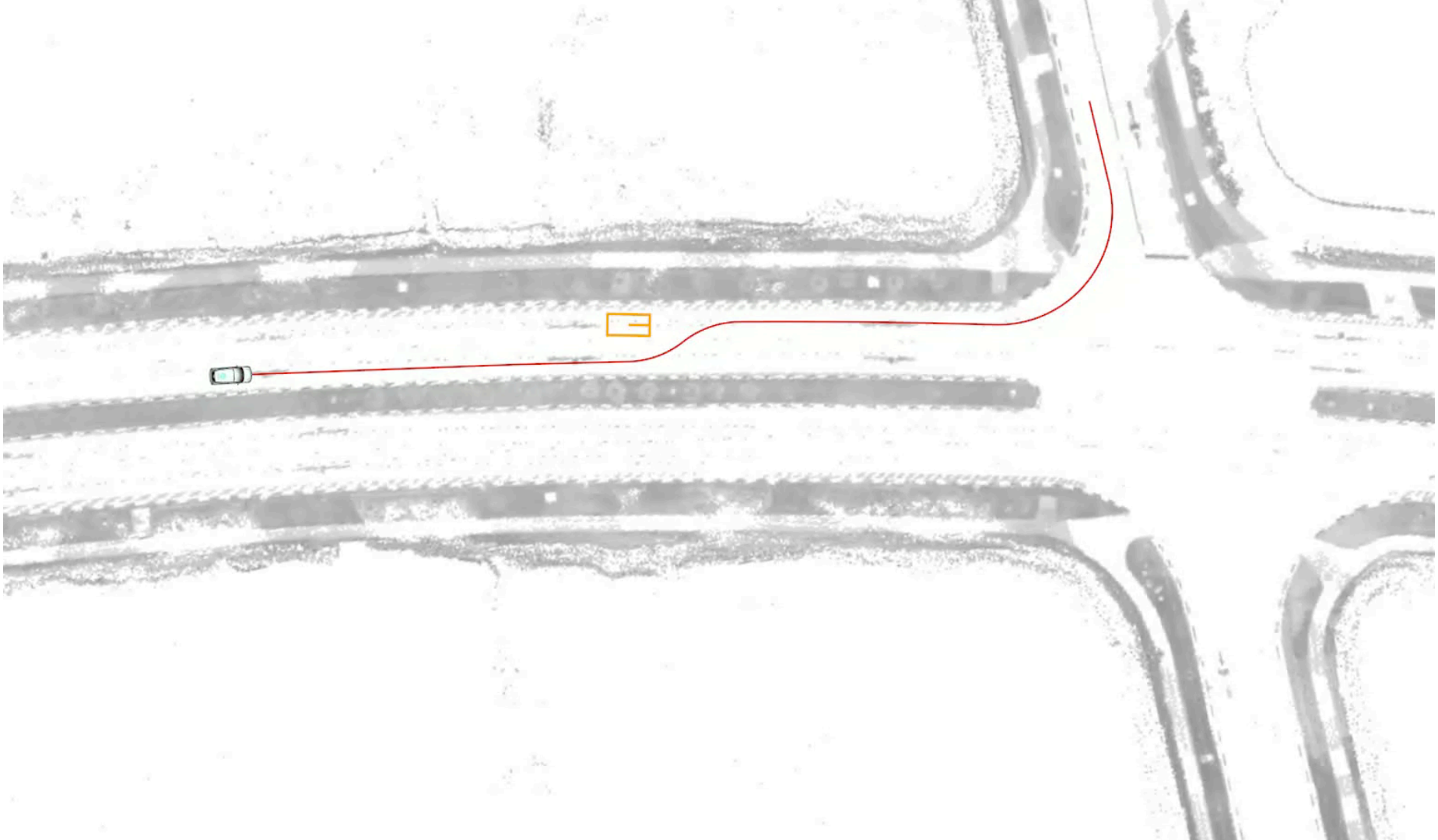
Fig 1. Draw two circles

Fig 2. Draw the rest of the damn Owl

Behavior specification is easy...

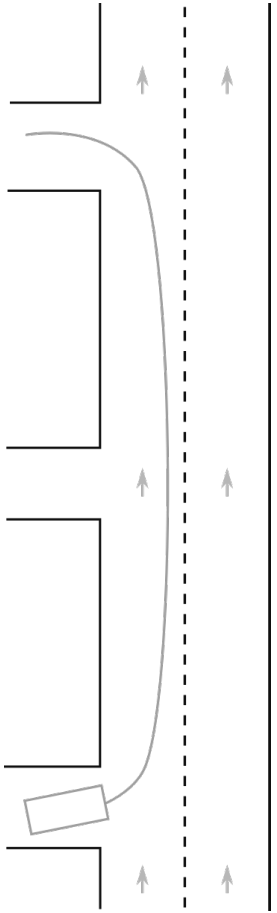
… unless it has to be precise.





Term Formalization

1. *The indicator should be activated after the **previous turn** has been passed*
2. *The indicator should be activated at least 3 seconds before **initiating** a turn*
3. *The indicator should be activated at least 30 meters before the turn is **made***



In Formal Methods…

Definition 2.1. Transition System (TS)

A *transition system* TS is a tuple $(S, Act, \rightarrow, I, AP, L)$ where

- S is a set of states,
- Act is a set of actions,
- $\longrightarrow \subseteq S \times Act \times S$ is a transition relation,
- $I \subseteq S$ is a set of initial states,
- AP is a set of atomic propositions, and
- $L : S \rightarrow 2^{AP}$ is a labeling function.

C. Baier and J.-P. Katoen, Principles of Model Checking (Representation and Mind Series). The MIT Press, 2008.

Even though automatic control of robots and teams of robots from high level specifications given as formulas of some temporal logic is useful and possible, several fundamental questions remain to be answered.

C. Belta, A. Bicchi, M. Egerstedt, E. Frazzoli, E. Klavins, and G. J. Pappas, Symbolic Planning and Control of Robot Motion, IEEE Robotics and Automation Magazine – special issue on Grand Challenges of Robotics, vol. 14, no. 1, pp. 61-71, 2007

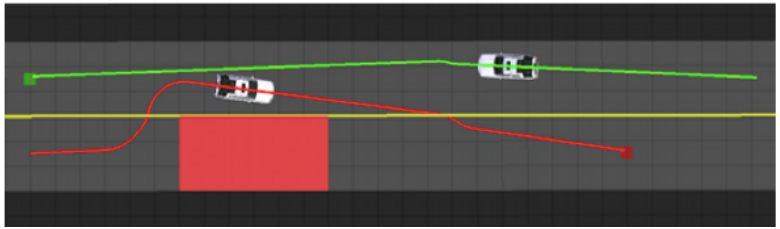
Minimum Violation Planning

- **No infeasibility**. The desired goal is guaranteed to be reached.
- Minimize a cost function that is representative of **the level of unsafety** with respect to the given safety rule.
  - Consider an ordered set of safety rules with priorities
  - The standard lexicographic ordering is used to compare the level of unsafety of trajectories

$$\lambda(w, \mathcal{A}) = \min_{I|\ \text{vanish}(w,I)\in L(\mathcal{A})} \sum_{i\in I} \varpi(\mathcal{A}).$$

$$\lambda(w, \Psi_i) = \sum_{\mathcal{A}_{i,j}\in\Psi_i} \lambda(w, \mathcal{A}_{i,j}),$$

$$\lambda(w, \mathbf{\Psi}) = \big(\lambda(w, \Psi_1), \ldots, \lambda(w, \Psi_n)\big)$$



L.I.R. Castro, P. Chaudhari, J. Tumova, S. Karaman, E. Frazzoli and D. Rus. Incremental Sampling-Based Algorithm for Minimum-Violation Motion Planning. In Proc. of IEEE International Conference on Decision and Control (CDC), 2013

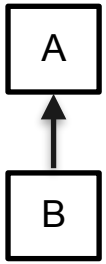
P. Chaudhari, T. Wongpiromsarn and E. Frazzoli. Incremental Synthesis of Minimum-Violation Control Strategies for Robots Interacting with External Agents. In American Control Conference (ACC), 2014.

APTIV

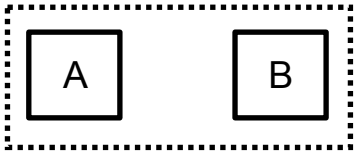
Rulebooks

A generalisation of minimum violation planning

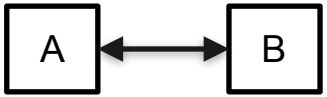
1. For autonomous vehicle, a **realization** is a world trajectory
2. A **rule** is a function on realizations and measures the degree of violation of any given realisation
3. A **rulebook** is a pre-ordered set of rules.



Rule A is more important than Rule B

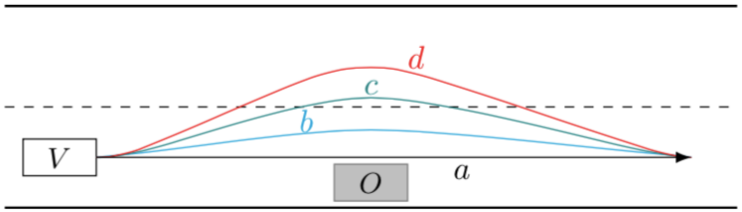


Rule A and Rule B are incomparable. The implementation can choose whether A or B is more important.

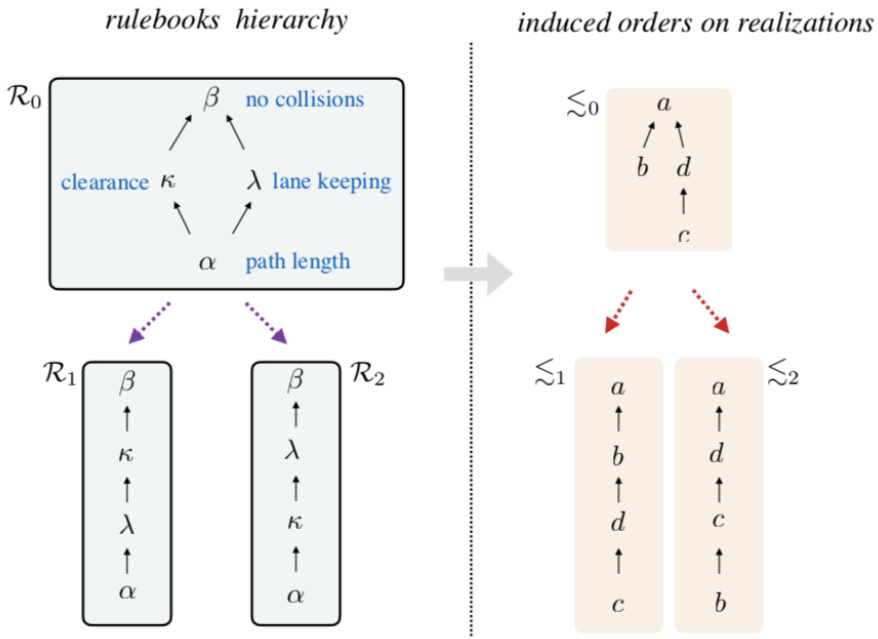


Rule A and Rule B are of the same rank

Behavior Specification using Rulebooks

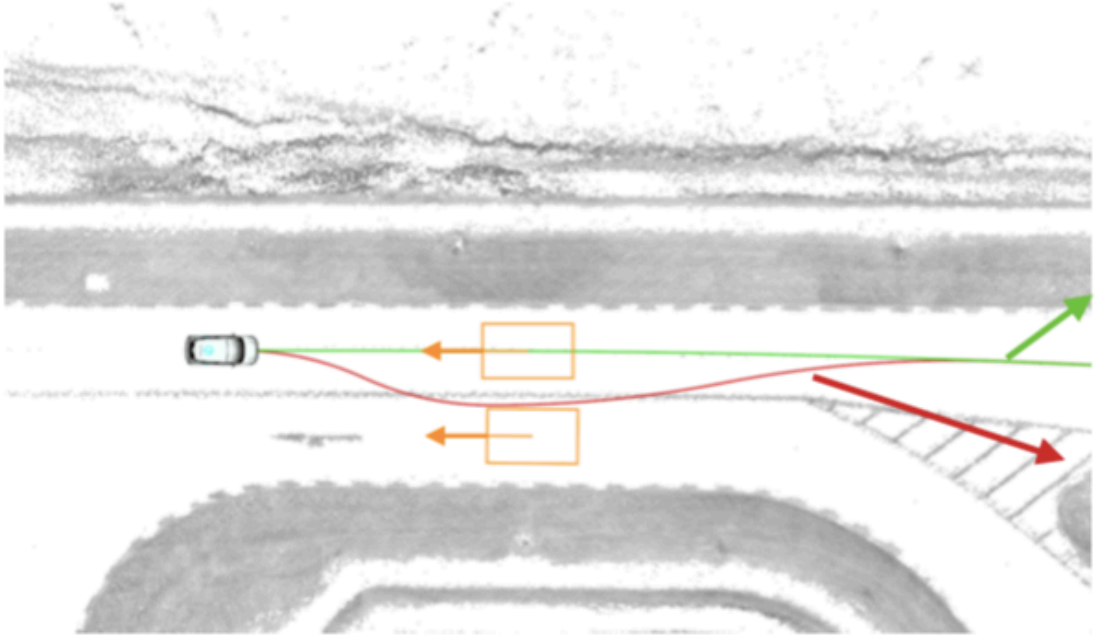


- **Partial specification** as a base for distinct jurisdictions
- Allow iterative specification refinement, including **priority refinement**, **rule aggregation** and **rule augmentation**



APTIV

Example: Liability-Aware Planning



$\mathcal{R}_b$

no collisions at fault

↑

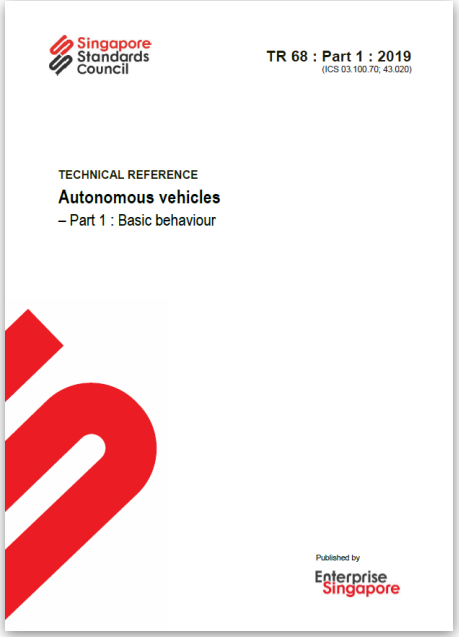
no collisions

$\mathcal{R}_a$

no collisions

Singapore Example: Technical Reference

- Singapore's technical recommendations for AV development, TR 68, released in January 2019
- Eventually, the TR will become the **SG Standard**
- Encodes the idea of minimum violation planning and rulebooks



APTIV


0.0 / 0.0 m/s
0.0 km/h
M P A P


4.0 / 5.7 m/s
14.5 km/h
M P A D

Behaviour Specifications of Autonomous Vehicles

Nok Wongpiromsarn

October 3, 2019

Contributions by
A. Censi, K. Slutsky, J. Fu, E. Frazzoli