Search-based Test-Case Generation by Monitoring Responsibility Safety Rules

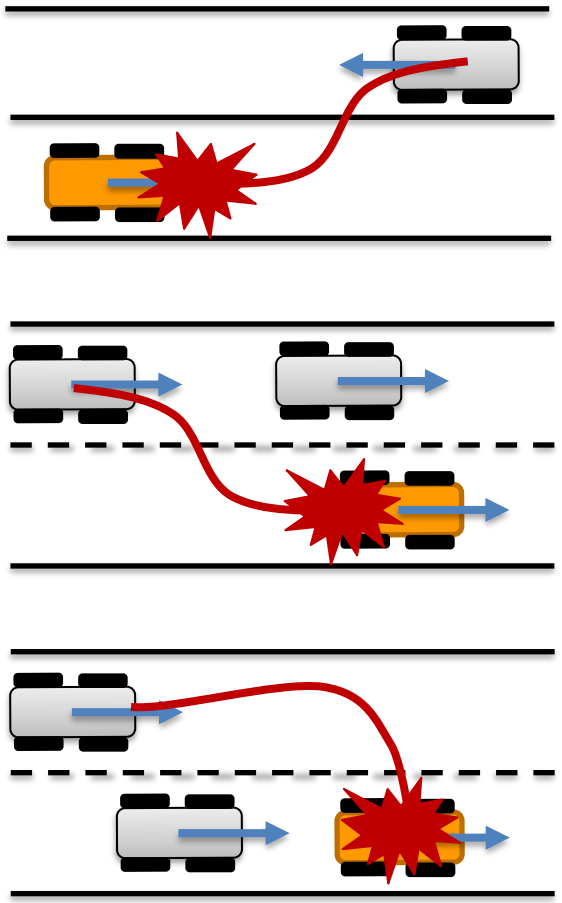
Mohammad Hekmatnejad, *Bardh Hoxha, and* ***Georgios Fainekos***
September 20-23, 2020

ITSC 2020

What is the challenge in open environment testing?

Challenge: we drive optimistically!

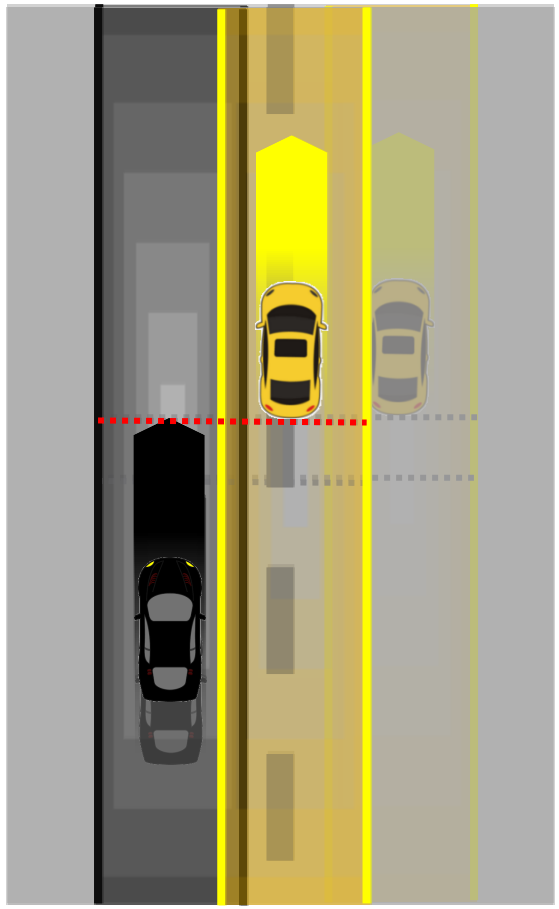
Car crashing onto a Waymo AV in autonomous mode in Chandler, AZ



Our claim: We need to detect and robustify "boundary" situations, i.e., we need **adversaries** to exercise the boundary behaviors between safe and unsafe scenarios.

One way to ignore such scenarios: *Responsibility Sensitive Safety Rules*[1]

- Responsibility Sensitive Safety (RSS) Rules developed by Intel Mobileye to capture safe driver behavior for automated driving systems
  - Alternative viewpoint: when an ADS should not be blamed for an accident



Laterally Unsafe

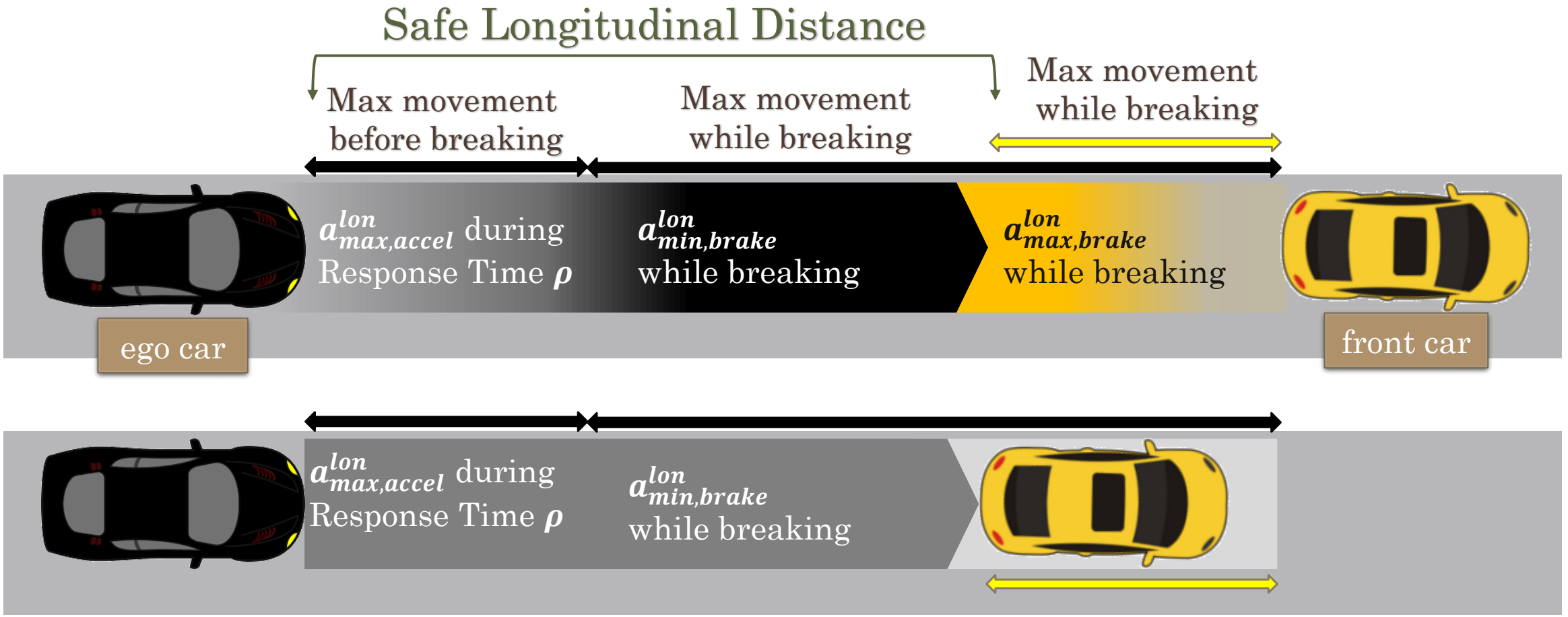
- How to use RSS in testing
  - As guidance for optimal stochastic sampling of test scenarios
  - As constraints for measuring the safety robustness of controllers in ADS

"… *before the Danger Threshold time there was a safe longitudinal distance, in an on coming scenario, hence the ego car should brake longitudinally.*"

[1] S. Shalev-Shwartz, S. Shammah, and A. Shashua, "**On a formal model of safe and scalable self-driving cars**," arXiv:1708.06374v6, 2018.

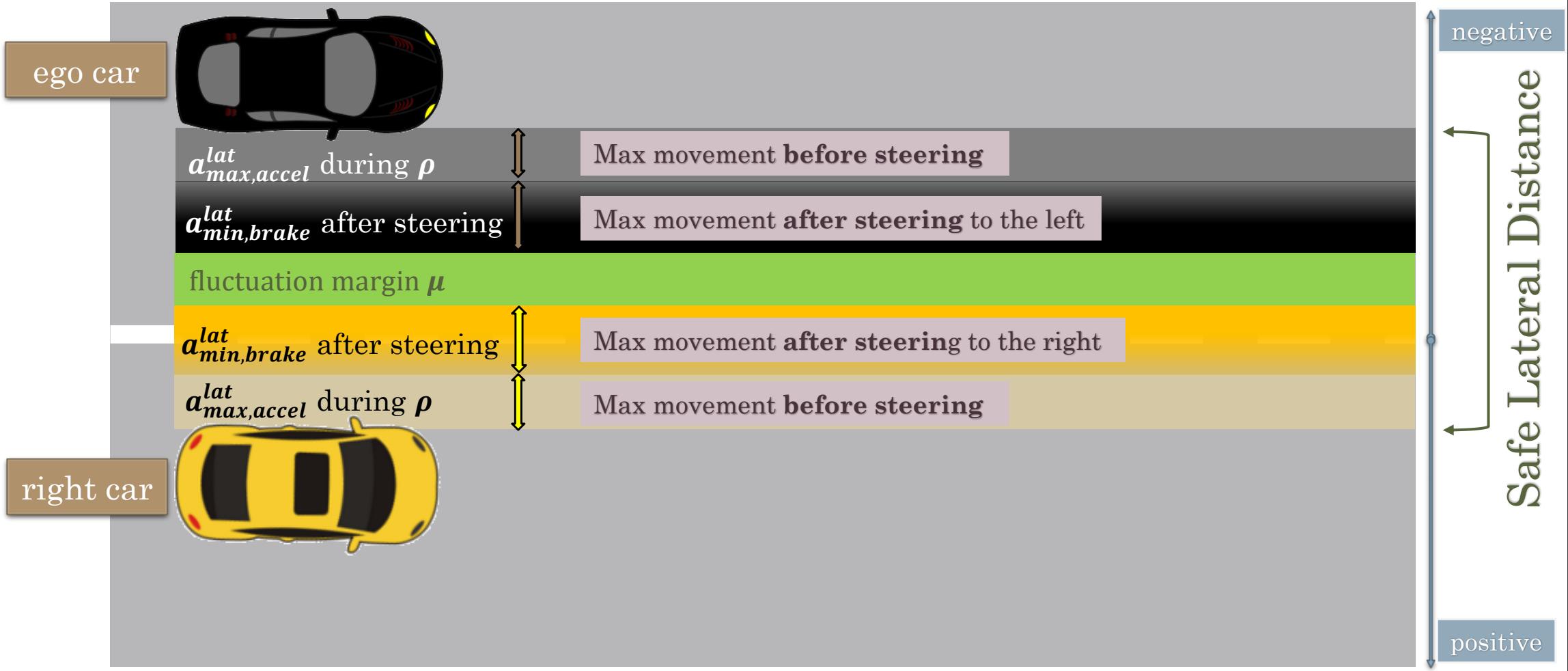
Safe Longitudinal Distance in One-Way Traffic

All cars move at the same direction from left to the right



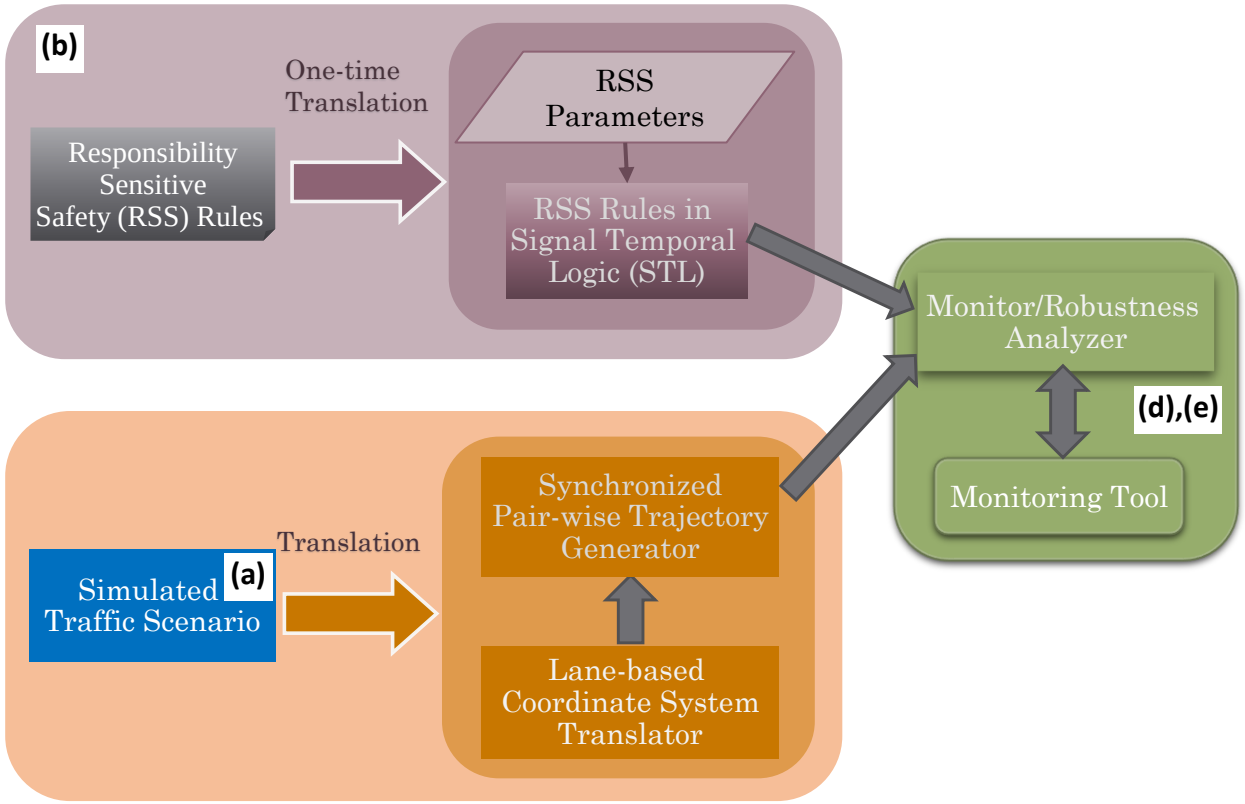
Safe Lateral Distance in One-Way Traffic

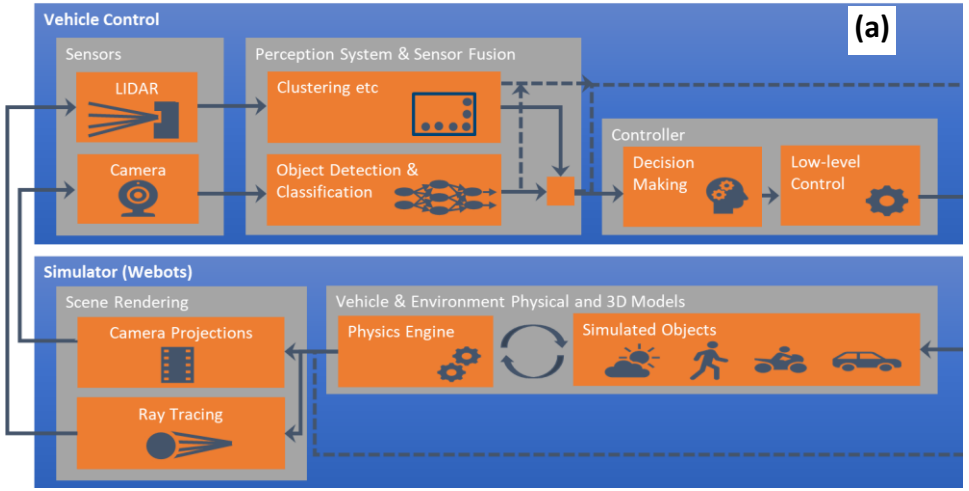
All cars move at the same direction from left to the right

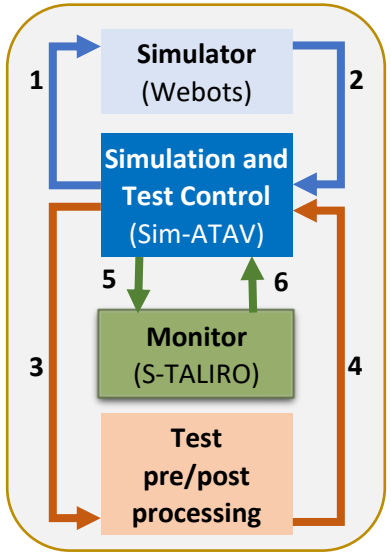


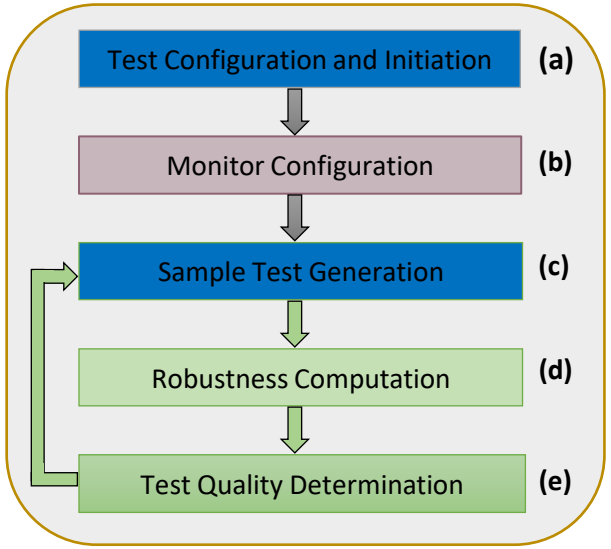
Solution Architecture

Tuncali et al. Requirements-driven Test Generation for Autonomous Vehicles with Machine Learning Components, IEEE Transactions on Intelligent Vehicles 2018 (arXiv 1908.01094)









Hekmatnejad et al, Encoding and Monitoring Responsibility Sensitive Safety Rules for Automated Vehicles in Signal Temporal Logic, MEMOCODE 2019

RSS rules in STL for Test Generation

Collision Avoidance Specification (CAS)

$$\varphi_{cas} \equiv \square\neg(dx^{a1}_{ego} < \delta_x \wedge dy^{a1}_{ego} < \delta_y \wedge dx^{a2}_{ego} < \delta_x \wedge dx^{a2}_{ego} < \delta_y)$$

Responsibility Sensitive Safety Specification (RSS)

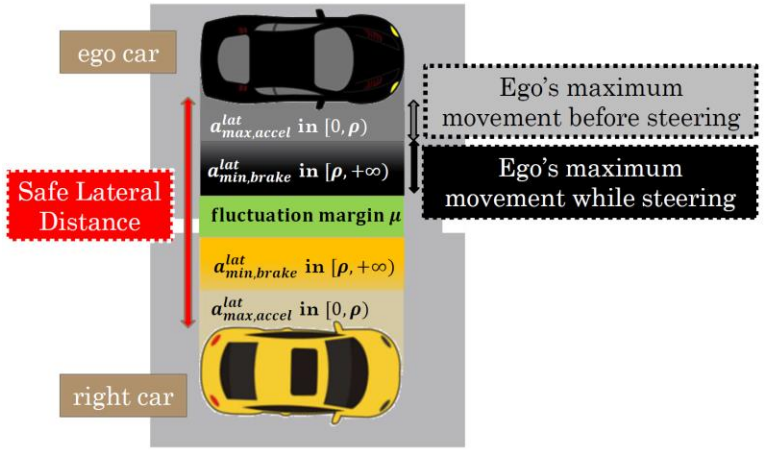
$$\varphi^{lat,lon}_{resp} \equiv \varphi^{lon} \wedge \varphi^{lat} \wedge \varphi^{lat,lon} \wedge \varphi^{\neg lat,\neg lon}$$

- $\varphi^{lon} \equiv \square\left(\left(\neg S^{lat}_{l,r} \wedge S^{lon}_{b,f} \wedge\circ \left(\neg S^{lat}_{l,r} \wedge \neg S^{lon}_{b,f}\right)\right) \rightarrow\circ \boldsymbol{P^{lon}_{lat}}\right)$
- $\varphi^{lat} \equiv \square\left(\left(\neg S^{lon}_{b,f} \wedge S^{lat}_{l,r} \wedge\circ \left(\neg S^{lon}_{b,f} \wedge \neg S^{lat}_{l,r}\right)\right) \rightarrow\circ \boldsymbol{P^{lat}_{lon}}\right)$
- $\varphi^{lat,lon} \equiv \square\left(\left(S^{lat}_{l,r} \wedge S^{lon}_{b,f} \wedge\circ \left(\neg S^{lat}_{l,r} \wedge \neg S^{lon}_{b,f}\right)\right) \rightarrow\circ \left(\boldsymbol{P^{lon}_{lat}} \vee \boldsymbol{P^{lat}_{lon}}\right)\right)$
- $\varphi^{\neg lat,\neg lon} \equiv \left(\left(\neg S^{lat}_{l,r} \wedge \neg S^{lon}_{b,f}\right) \rightarrow\circ \left(\boldsymbol{P^{lon}_{lat}} \vee \boldsymbol{P^{lat}_{lon}}\right)\right)$

Hekmatnejad et al, Encoding and Monitoring Responsibility Sensitive Safety Rules for Automated Vehicles in Signal Temporal Logic, MEMOCODE 2019

$$\boldsymbol{P^{lon}_{lat}} \equiv \left((S^{lat}_{l,r} \vee S^{lon}_{b,f})\bar{\mathcal{R}}_{[0,\rho)}(A^{lon}_{b,maxAcc})\right) \wedge \left((S^{lat}_{l,r} \vee S^{lon}_{b,f})\bar{\mathcal{R}}_{[\rho,+\infty)}(A^{lon}_{b,minBr})\right)$$

$$\boldsymbol{P^{lat}_{lon}} \equiv (P^{lat}_{0,\rho} \wedge P^{lat,1}_{\rho,\infty} \wedge P^{lat,2}_{\rho,\infty})$$



$$\boldsymbol{P^{lat}_{0,\rho}} \equiv (S^{lat}_{l,r} \vee S^{lon}_{b,f})\bar{\mathcal{R}}_{[0,\rho)}(A^{lat}_{l,,maxAcc})$$

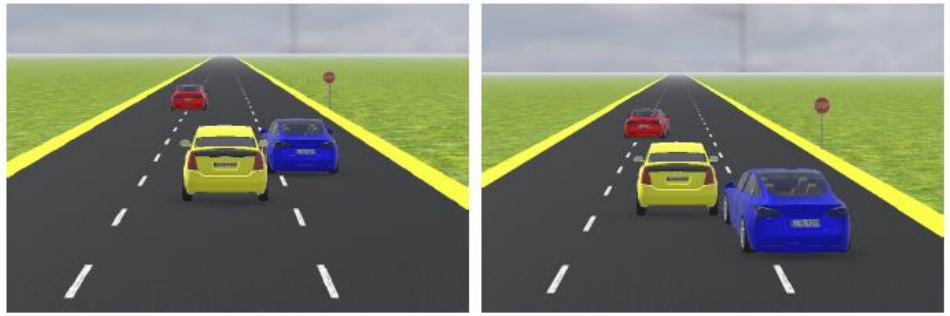
$$\boldsymbol{P^{lat,1}_{\rho,\infty}} \equiv (S^{lat}_{l,r} \vee S^{lon}_{b,f} \vee V^{lat}_{l,stop})\bar{\mathcal{R}}_{[\rho,+\infty)}(A^{lat}_{l,minBr})$$

$$\boldsymbol{P^{lat,2}_{\rho,\infty}} \equiv (S^{lat}_{l,r} \vee S^{lon}_{b,f})\bar{\mathcal{R}}_{[\rho,+\infty)}(V^{lat}_{l,stop} \rightarrow (S^{lat}_{l,r} \vee S^{lon}_{b,f})\bar{\mathcal{R}}(V^{lat}_{l,neg}))$$

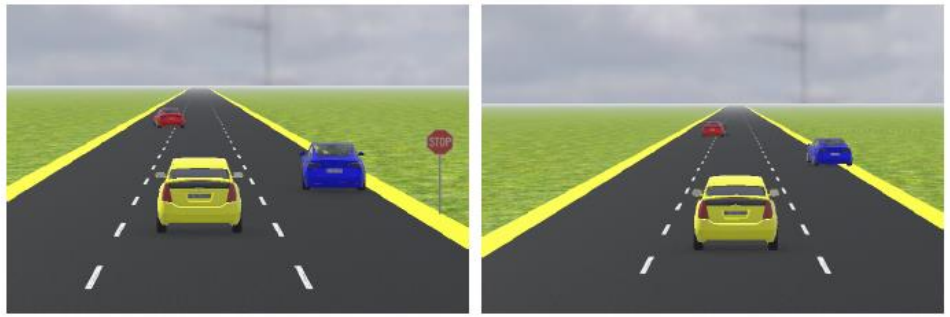
Test Scenario (case study)

- The yellow car is the ego car
  - Its initial position, orientation and speed are sampled through various methods (i.e., uniform random sampling or stochastic optimization)
- The blue and red cars are adversarial
  - All their initial conditions, plus their whole trajectory are generated using various methods

Test Scenario (Cont')



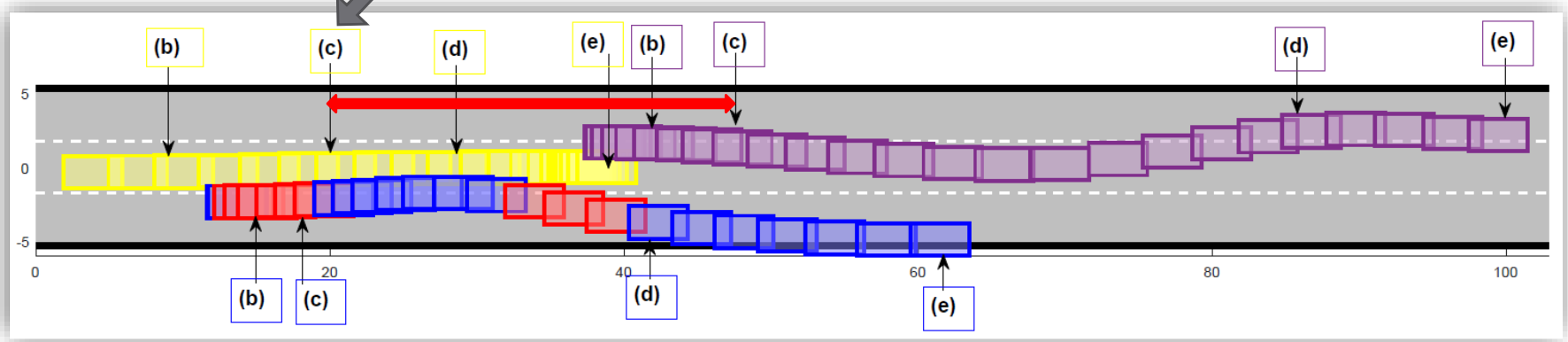
(b) first snapshot. (c) second snapshot.



(d) third snapshot. (e) forth snapshot.

The longitudinal reaction is modified to only cover the following car

$$\boldsymbol{P^{lon}_{lat}} \equiv \left((S^{lat}_{l,r} \vee S^{lon}_{b,f})\bar{\mathcal{R}}_{[0,\rho)}(A^{lon}_{b,maxAcc})\right) \wedge \left((S^{lat}_{l,r} \vee S^{lon}_{b,f})\bar{\mathcal{R}}_{[\rho,+\infty)}(A^{lon}_{b,minBr})\right)$$



Experiments and Results

The Necessity of RSS in Testing

- 1000 test scenarios
- 23% RSS violation vs 60% CAS violation
- 19 tests did not lead to accident but violated RSS

Improving Search-based Testing through RSS

- falsifying the CAS specification
- 1000 test scenarios
- finds more dangerous test-driving scenarios
- 60% RSS violation vs 98% CAS violation
- 20 tests did not lead to accident but violated RSS

- falsifying the RSS specifications
- 350 test scenarios
- finds more relevant test-driving scenarios
- 16% RSS violation vs 85% CAS violation
- 1 test did not lead to accident but violated RSS
- classify test scenarios based on their violated constraints

predicates	# of violations	description
$S^{lon}_{b,f}$	2	safe longitudinal distance
$S^{lat}_{l,r}$	23	safe lateral distance
$A^{lat}_{l,maxAcc}$	67	maximum allowed lateral acceleration
$A^{lat}_{l,minBr}$	0	minimum required lateral brake
$V^{lat}_{l,stop}$	68	zero μ−lateral velocity
$V^{lat}_{l,neg}$	0	non-positive μ−lateral velocity
$A^{lon}_{b,maxAcc}$	33	maximum allowed longitudinal acceleration
$A^{lon}_{b,minBr}$	36	minimum required longitudinal brake
Execution Statistics		
violation %	22.9%	falsified percentage using the RSS rules

predicates	# of violations	description
$S^{lon}_{b,f}$	2	safe longitudinal distance
$S^{lat}_{l,r}$	3	safe lateral distance
$A^{lat}_{l,maxAcc}$	13	maximum allowed lateral acceleration
$A^{lat}_{l,minBr}$	0	minimum required lateral brake
$V^{lat}_{l,stop}$	0	zero μ−lateral velocity
$V^{lat}_{l,neg}$	0	non-positive μ−lateral velocity
$A^{lon}_{b,maxAcc}$	35	maximum allowed longitudinal acceleration
$A^{lon}_{b,minBr}$	5	minimum required longitudinal brake
Execution Statistics		
violation %	16.5%	falsified percentage using the RSS rules

Conclusions

- We used the encoded formulas for automated test case generation for discovering control software bugs (our Sim-ATAV framework*)
  - We presented an automated and qualification-based method for generating driving test scenarios.
  - The generated tests could be used for discovering control software bugs in Automated Driving Systems (ADS).
  - Automatically extract vehicle trajectories from youtube videos! **

- Future Work
  - Translating the RSS rules for other needed driving scenarios such as cross sections
  - Use the extended translation of the RSS model in our search-based test-case generator

* C. E. Tuncali, G. Fainekos, H. Ito, and J. Kapinski, "***Simulationbased adversarial test generation for autonomous vehicles with machine learning components***," in IEEE Intelligent Vehicles Symposium (IV), 2018.

** Bashetty, Sai Krishna, Heni Ben Amor, and Georgios Fainekos. ***"DeepCrashTest: Turning Dashcam Videos into Virtual Crash Tests for Automated Driving Systems."*** arXiv preprint arXiv:2003.11766 (2020).

Questions?

Georgios Fainekos
fainekos@asu.edu
https://www.public.asu.edu/~gfaineko/

Mohammad Hekmatnejad
mhekmatn@asu.edu

Bardh Hoxha
bardh.hoxha@toyota.com

Acknowledgements

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.
NSF awards 1350420 and 1361926

CENTER FOR EMBEDDED SYSTEMS
an NSF Industry/University Cooperative Research Center

Erkan Tuncali
Former labmate

Auxiliary Slides

Metric Temporal Logic* (MTL)

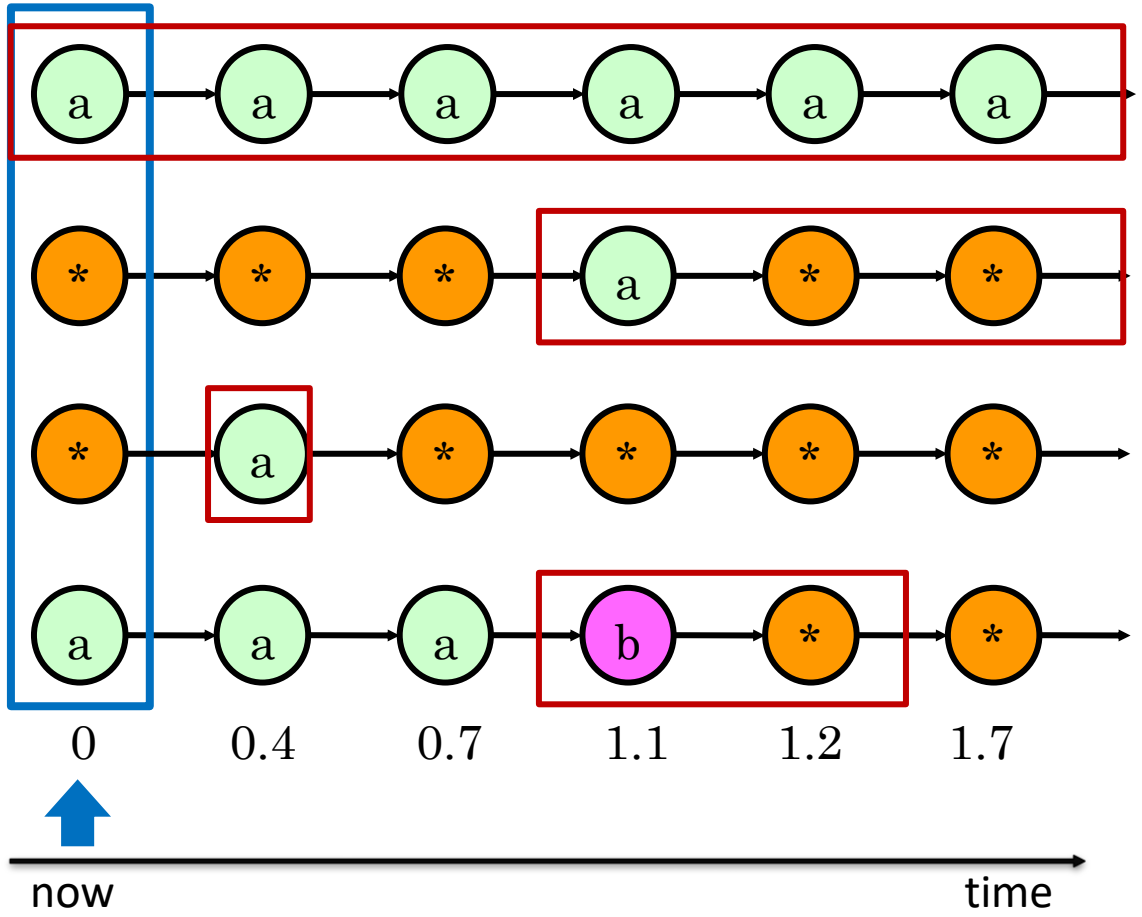
- Syntax: $\phi ::= \top |p| \neg\phi \mid \phi_1 \vee \phi_2 | \Box_I \phi | \Diamond_I \phi | \bigcirc \phi | \phi_1 U_I \phi_2 | \phi_1 R_I \phi_2$
- Semantics:

$G_{[0,\infty)} a \equiv \Box_{[0,\infty)} a$ - Always a

$F_{[1,3]} a \equiv \Diamond_{[1,3]} a$ - Eventually a

$X a \equiv \bigcirc a$ - Next a

$a \; U_{[1,1.5]} \; b$ -a until b



* R. Koymans "Specifying real-time properties with metric temporal logic" Real-Time Systems, 2(4):255–299, 1990

Metric Temporal Logic* (MTL)

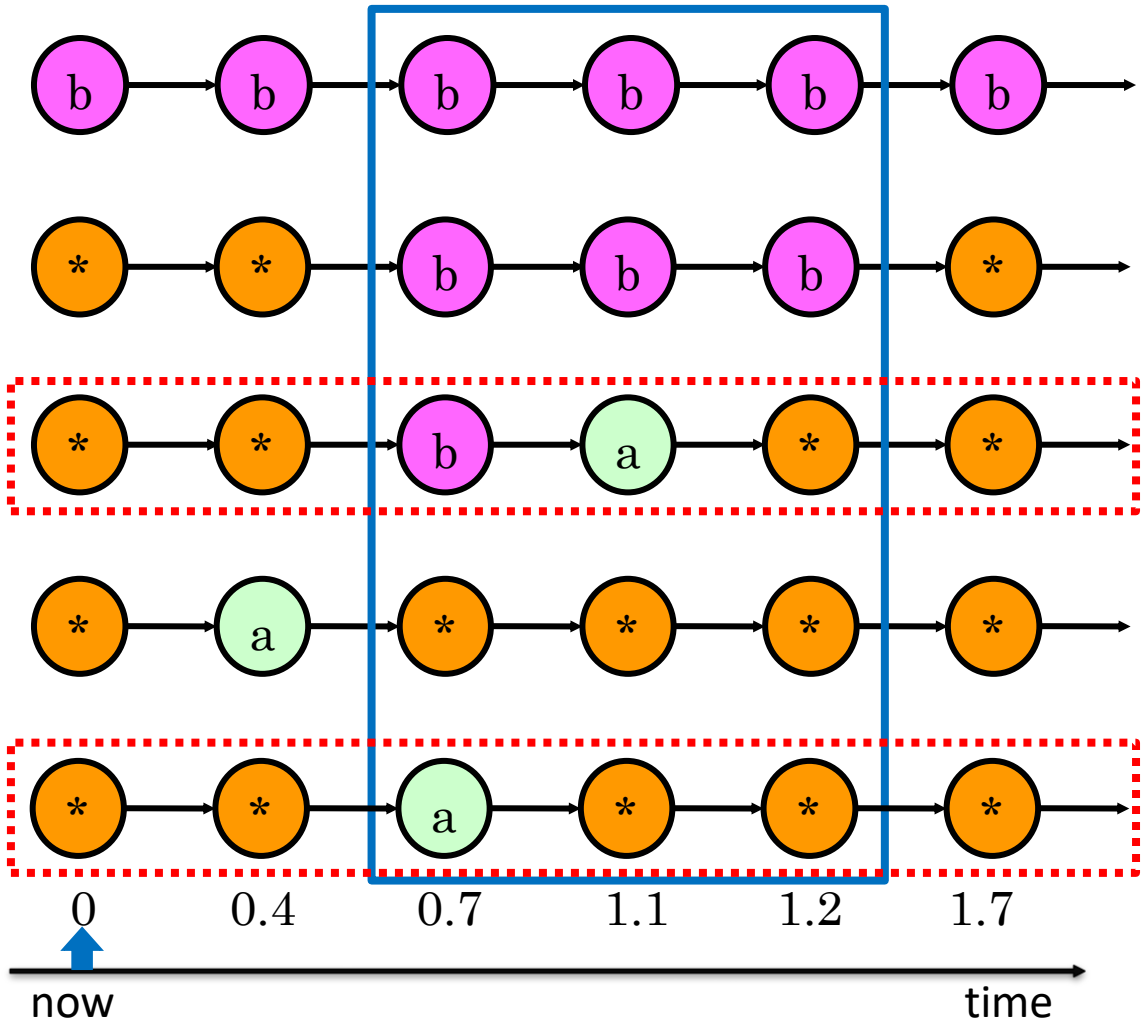
- Syntax: $\phi ::= \top |p| \neg\phi \mid \phi_1 \vee \phi_2 | \Box_I \phi | \Diamond_I \phi | \bigcirc \phi | \phi_1 U_I \phi_2 | \phi_1 R_I \phi_2$
- Semantics:

non-strict release

$a \overline{R}_{[0.5,1.5]} b$ - a release b

Satisfy b in the interval [0.5,1.5] unless a has happened in the past.

The requirement to satisfy b in the interval [0.5,1.5] is released when a was true in the past.



* R. Koymans "Specifying real-time properties with metric temporal logic" Real-Time Systems, 2(4):255–299, 1990

Longitudinal Safety Requirements

- **Longitudinal Safety Requirement for Ego vehicle:**

$$\varphi_{resp}^{lon} \equiv \square\left(\left(S_{b,f}^{lon} \wedge \circ \neg S_{b,f}^{lon}\right) \rightarrow \circ\, \boldsymbol{P^{lon}}\right)$$

** Hekmatnejad et al, Encoding and Monitoring Responsibility Sensitive Safety Rules for Automated Vehicles in Signal Temporal Logic, MEMOCODE 2019*

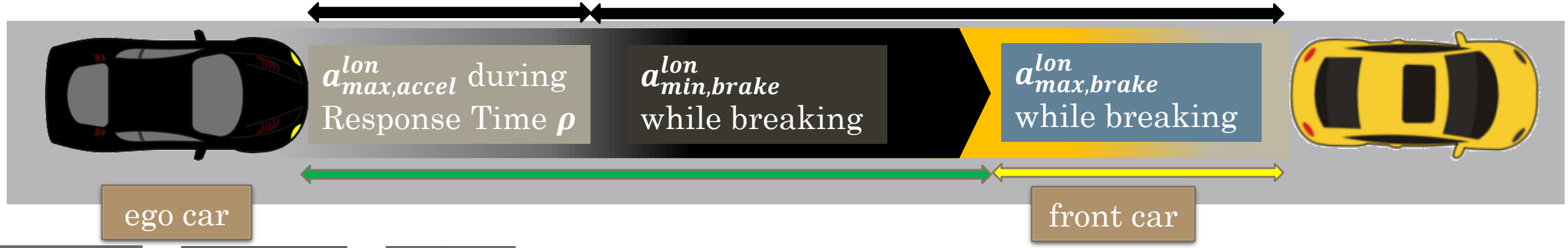
$$\boldsymbol{P^{lon}} \equiv \left(S_{b,f}^{lon}\, \bar{\mathcal{R}}_{[0,\rho)}\left(A_{b,maxAcc}^{lon} \wedge A_{f,maxBr}^{lon}\right)\right) \wedge \left(S_{b,f}^{lon}\, \bar{\mathcal{R}}_{[\rho,+\infty)}\left(A_{b,minBr}^{lon} \wedge A_{f,maxBr}^{lon}\right)\right)$$

$$S_{b,f}^{lon} \equiv \gamma(y_f, x_f)_y - \gamma(y_b, x_b)_y - d_{min,lon} > 0$$

$A_{b,maxAcc}^{lon} \equiv a_b^{lon} \leq a_{max,accel}^{lon}$

$A_{b,minBr}^{lon} \equiv a_b^{lon} \leq -a_{min,brake}^{lon}$

$A_{f,maxBr}^{lon} \equiv a_f^{lon} \geq -a_{max,brake}^{lon}$



Lateral Safety Requirements

- **Lateral Safety Requirement for Ego vehicle:**

$$\varphi_{resp}^{lat} \equiv \square\left(\left(S_{l,r}^{lat} \wedge \circ \neg S_{l,r}^{lat}\right) \rightarrow \circ\, \boldsymbol{P^{lat}}\right)$$

$$\boldsymbol{P^{lat}} \equiv \left(P_{o,\rho}^{lat} \wedge P_{\rho,\infty}^{lat,1} \wedge P_{\rho,\infty}^{lat,2}\right)$$

$$P_{o,\rho}^{lat} \equiv S_{l,r}^{lat}\, \bar{\mathcal{R}}_{[0,\rho)}\left(A_{l,maxAccel}^{lat} \wedge A_{r,maxAccel}^{lat}\right)$$

$$P_{\rho,\infty}^{lat,1} \equiv \left(\left(S_{l,r}^{lat} \vee V_{l,stop}^{lat}\right)\bar{\mathcal{R}}_{[\rho,+\infty)} A_{l,minBrake}^{lat}\right) \wedge \left(\left(S_{l,r}^{lat} \vee V_{r,stop}^{lat}\right)\bar{\mathcal{R}}_{[\rho,+\infty)} A_{r,minBrake}^{lat}\right)$$

$$P_{\rho,\infty}^{lat,2} \equiv \left(S_{l,r}^{lat}\, \bar{\mathcal{R}}_{[\rho,+\infty)}\left(V_{l,stop}^{lat} \rightarrow S_{l,r}^{lat}\, \bar{\mathcal{R}}\, V_{l,npos}^{lat}\right)\right) \wedge \left(S_{l,r}^{lat}\, \bar{\mathcal{R}}_{[\rho,+\infty)}\left(V_{r,stop}^{lat} \rightarrow S_{l,r}^{lat}\, \bar{\mathcal{R}}\, V_{r,nneg}^{lat}\right)\right)$$

$$S_{l,r}^{lat} \equiv \gamma(y_r, x_r)_\alpha - \gamma(y_l, x_l)_\alpha - d_{min,lat} > 0$$

$$V_{l,stop}^{lat} \equiv v_l^{\mu-lat} = 0,\ V_{r,stop}^{lat} \equiv v_r^{\mu-lat} = 0$$

$$V_{l,npos}^{lat} \equiv v_l^{\mu-lat} \leq 0,\ V_{r,nneg}^{lat} \equiv v_r^{\mu-lat} \geq 0$$

(i) Computed at signal level
(ii) Formalized as TPTL formula

$$A_{l,maxAccel}^{lat} \equiv |a_l^{lat}| \leq a_{max,accel}^{lat}$$

$$A_{l,minBrake}^{lat} \equiv a_l^{lat} \leq -a_{min,brake}^{lat}$$

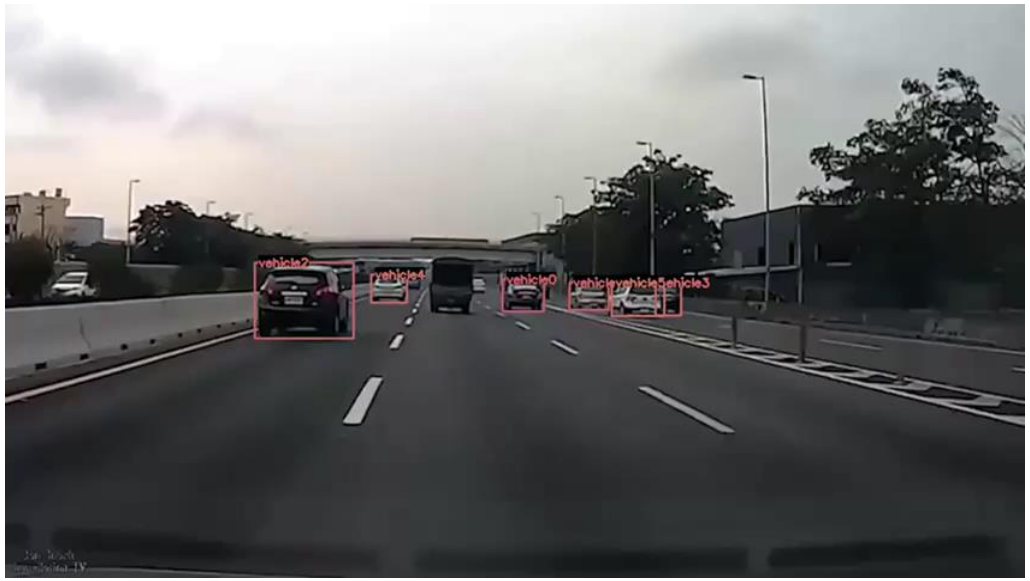
$$A_{r,minBrake}^{lat} \equiv a_r^{lat} \geq a_{min,brake}^{lat}$$

$$A_{r,maxAccel}^{lat} \equiv |a_r^{lat}| \leq a_{max,accel}^{lat}$$

** Hekmatnejad et al, Encoding and Monitoring Responsibility Sensitive Safety Rules for Automated Vehicles in Signal Temporal Logic, MEMOCODE 2019*

Can we initialize interesting scenarios quickly?

Automatically extract vehicle trajectories from youtube videos!



https://www.youtube.com/watch?v=CZHvce5wjPE

Bashetty, Sai Krishna, Heni Ben Amor, and Georgios Fainekos. "DeepCrashTest: Turning Dashcam Videos into Virtual Crash Tests for Automated Driving Systems." arXiv preprint arXiv:2003.11766 (2020).