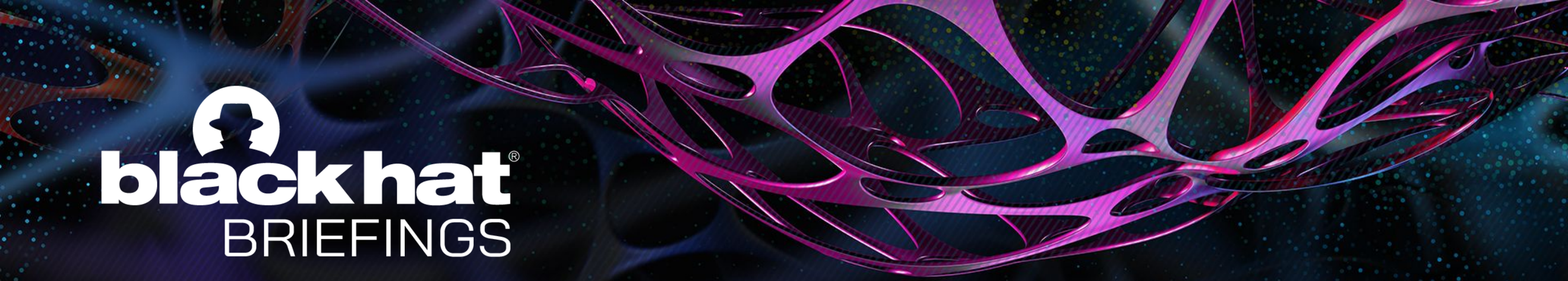


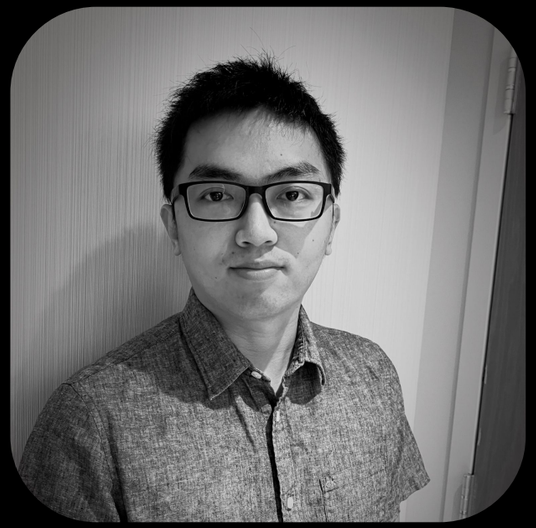
AUGUST 6-7, 2025
MANDALAY BAY / LAS VEGAS

Adversarial Fuzzer for Teleoperation Commands:

Evaluating Autonomous Vehicle Resilience

Zhisheng Hu, Shanit Gupta, Cooper de Nicola

About Us



Zhisheng Hu
Product Security Engineer

Shanit Gupta
Director of Product Security

⚠ Disclaimer

All tests were conducted in **simulation** or **tightly controlled test environment**. Collisions occurred only in **simulation**. Results are based on outdated software versions.

What is Teleoperation?

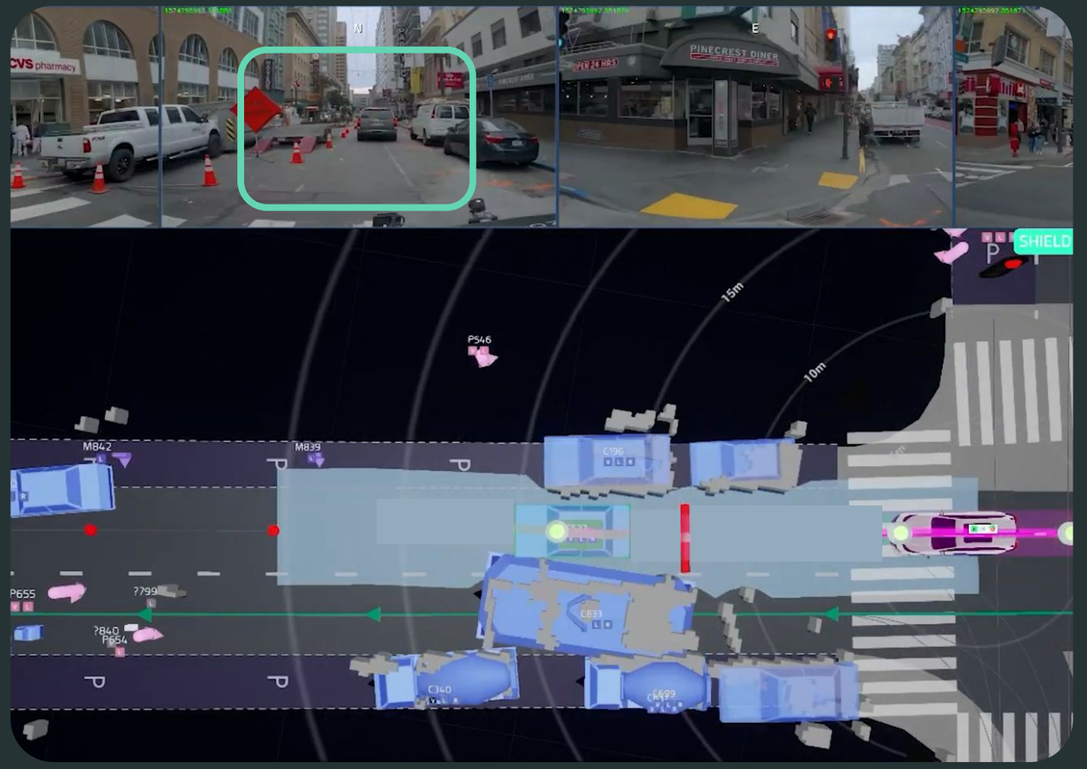

black hat
BRIEFINGS
P293
P212
P181
P492
P893
15m
10m
5m
SHIELD | ACCEPTED | Path valid


black hat
BRIEFINGS
SHIELD | ACCEPTED | Path validated
15m
10m
5m
P293
P212
P181
P493
P893

Operations Center

Detect potential construction zone

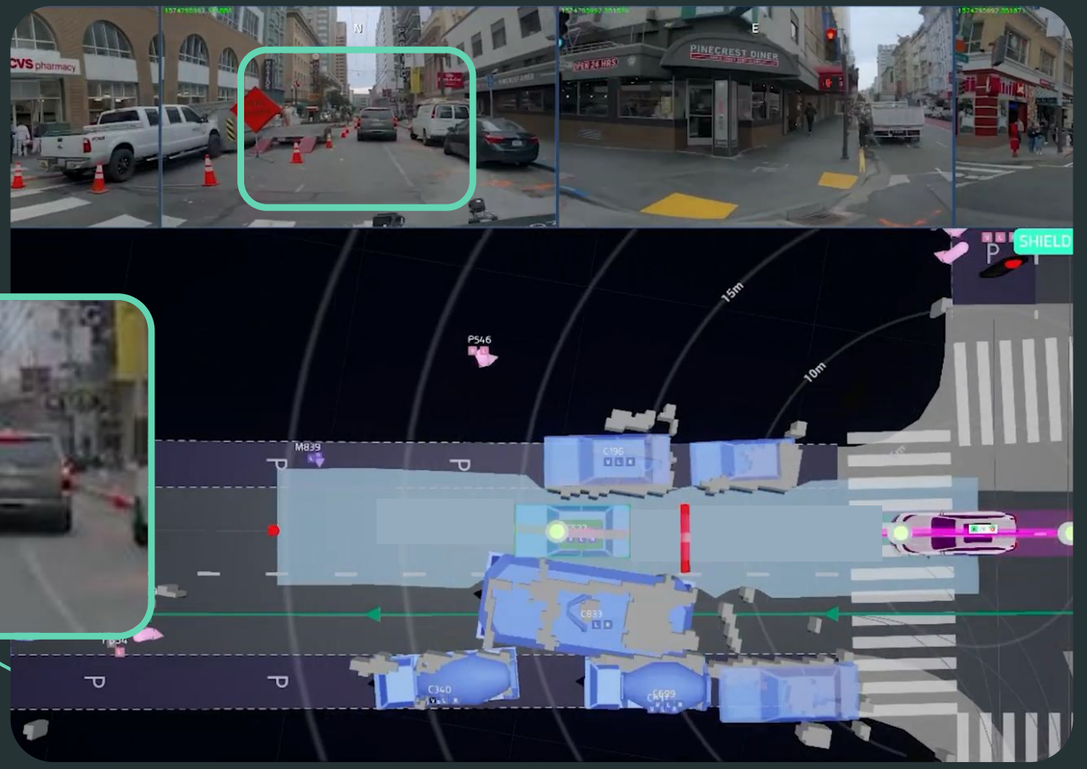
Vehicle



Operations Center

AI: Hey human, take a look. Is something in my way?

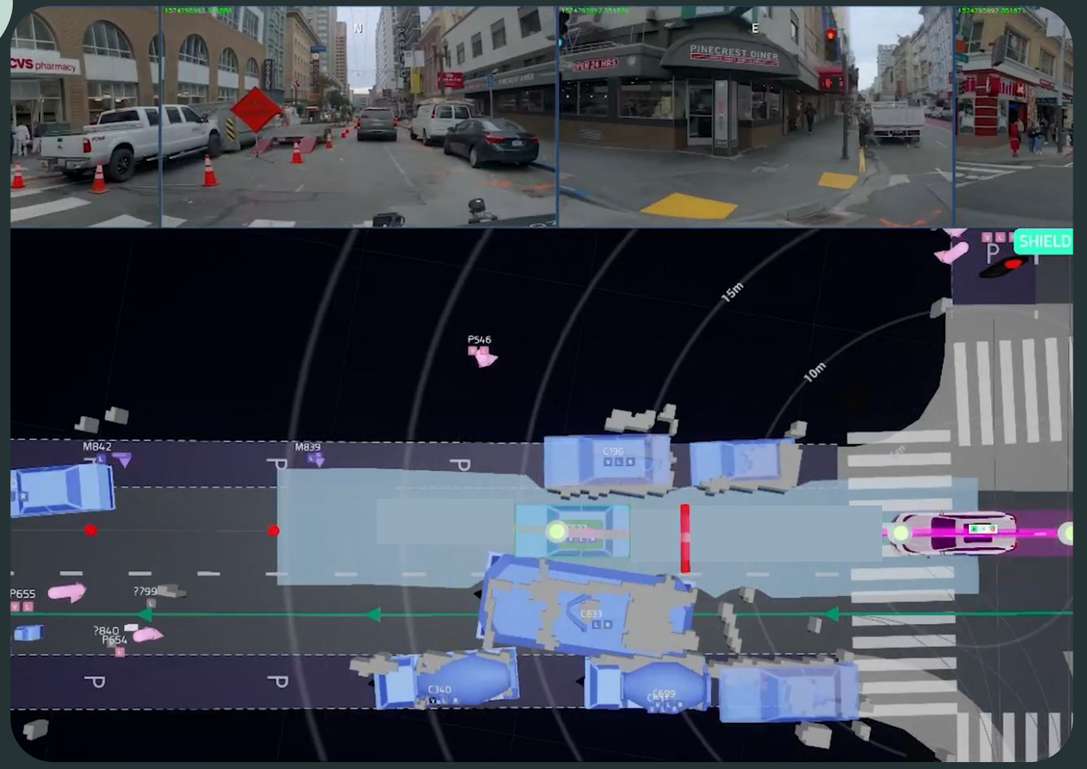
Vehicle



Operations Center

OP: Yes, lane shifted or closed

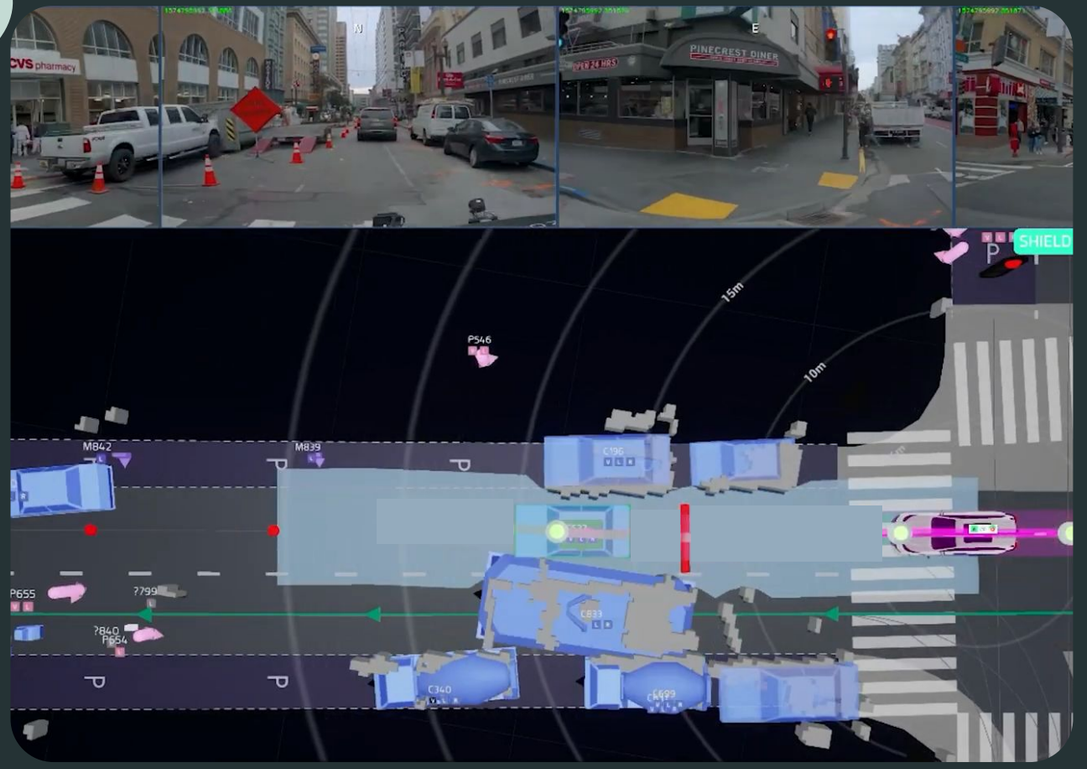
Vehicle



Operations Center

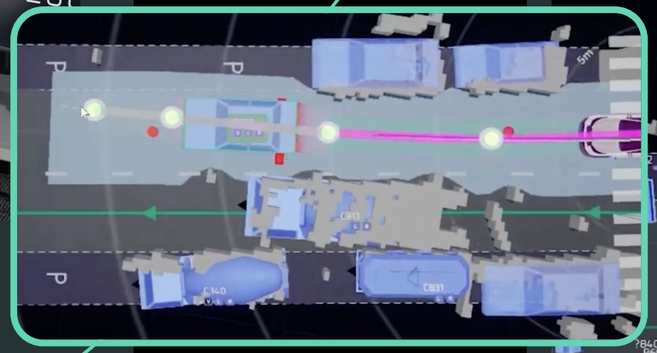
AI: Any suggestions?

Vehicle



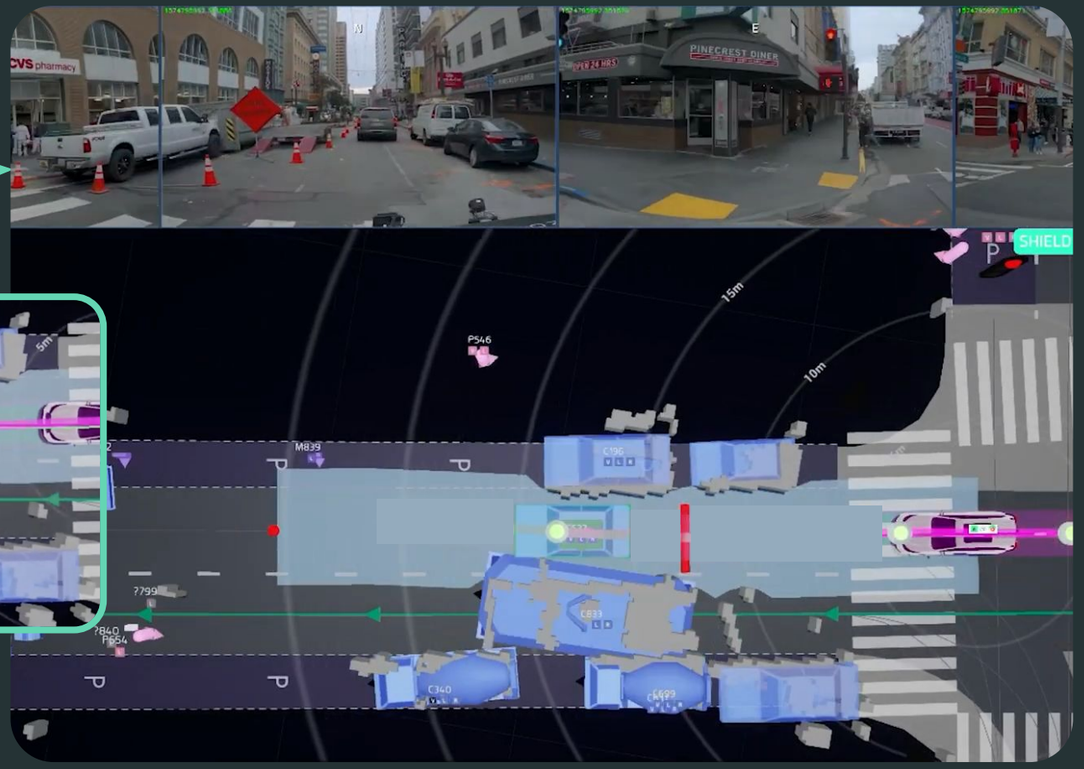
Operations Center

OP: Try this *suggestion*



Suggestion:
- **Waypoints**
- Stop
...

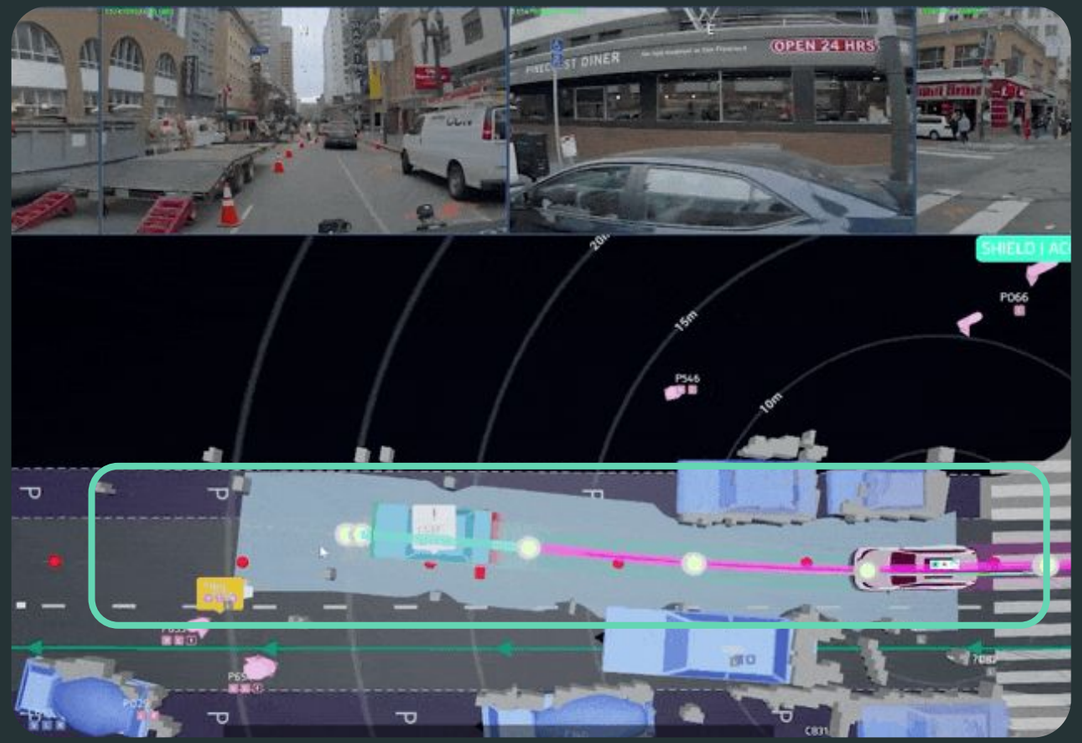
Vehicle



Operations Center

AI: Nice, let me try it.

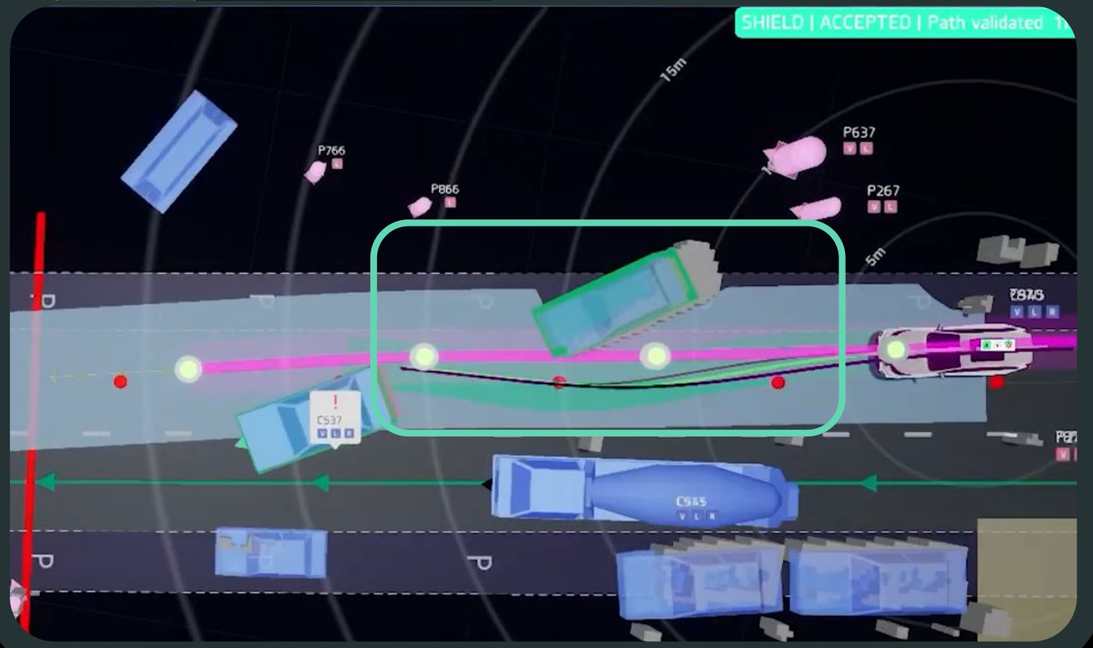
Vehicle



Operations Center

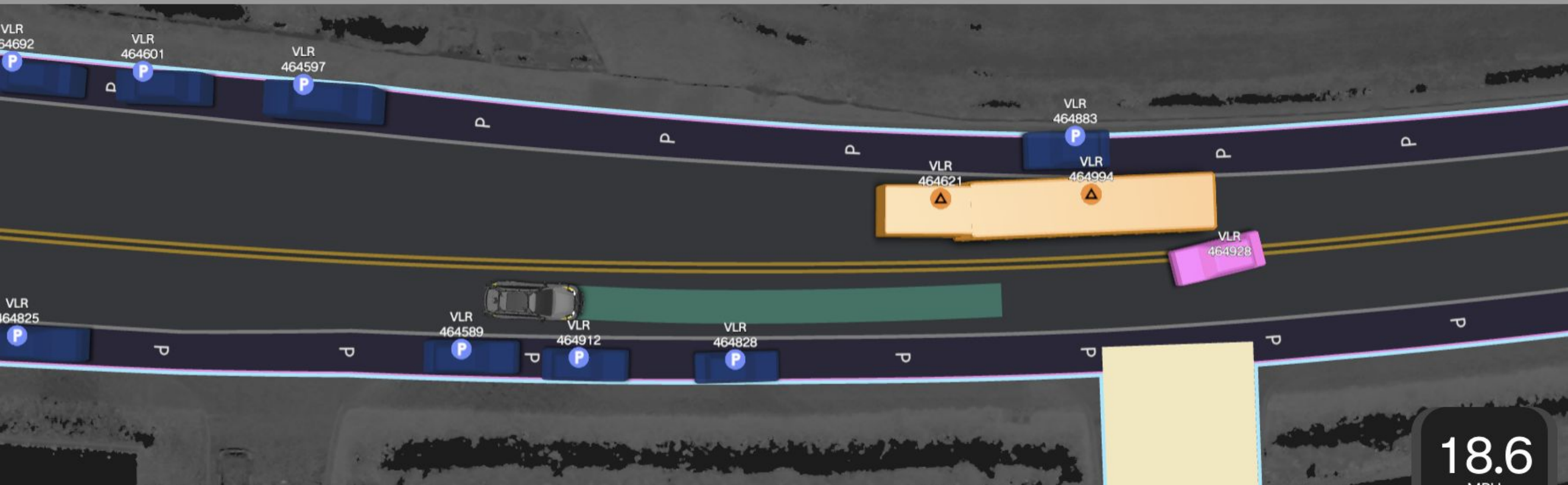
AI: Don’t worry, I am still in full autonomy

Vehicle

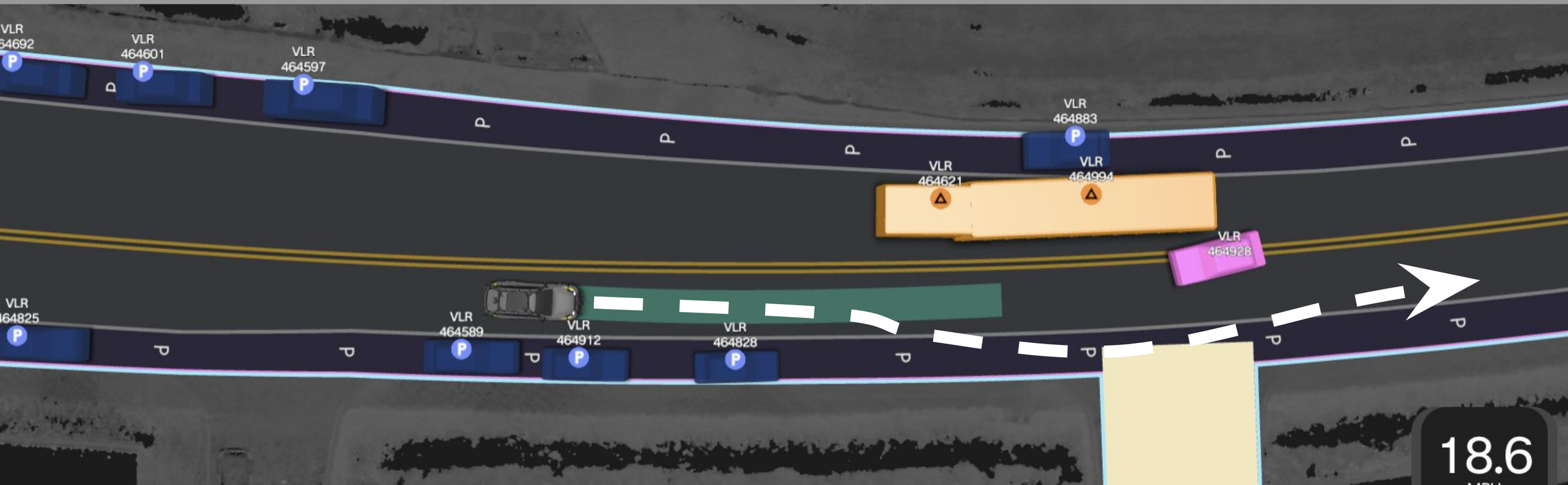


How to Show Teleoperation is Working Safely

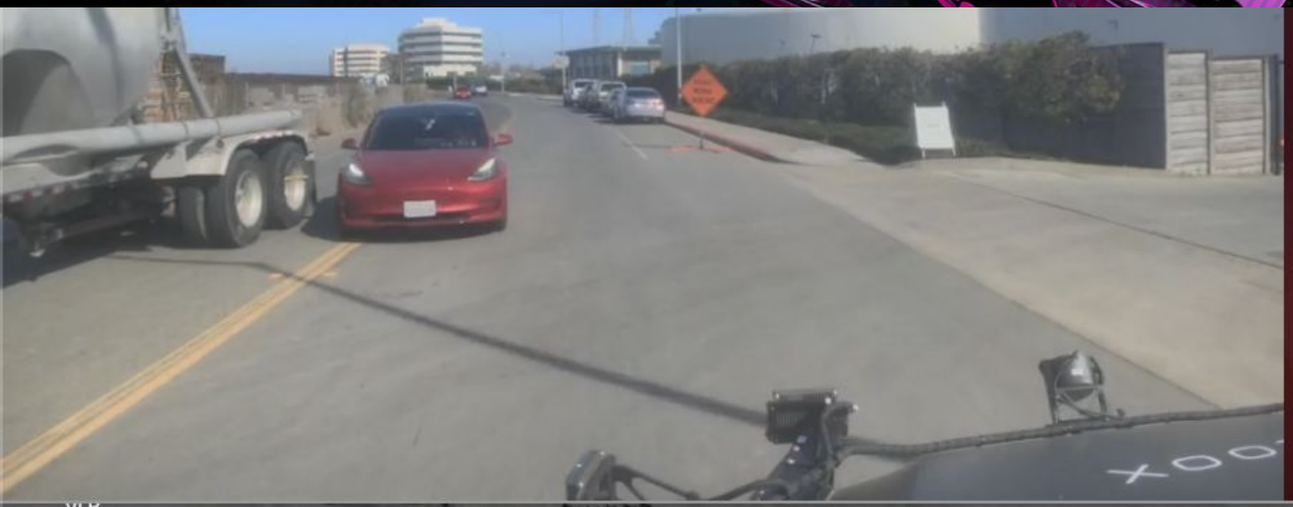
Implement real-world test case

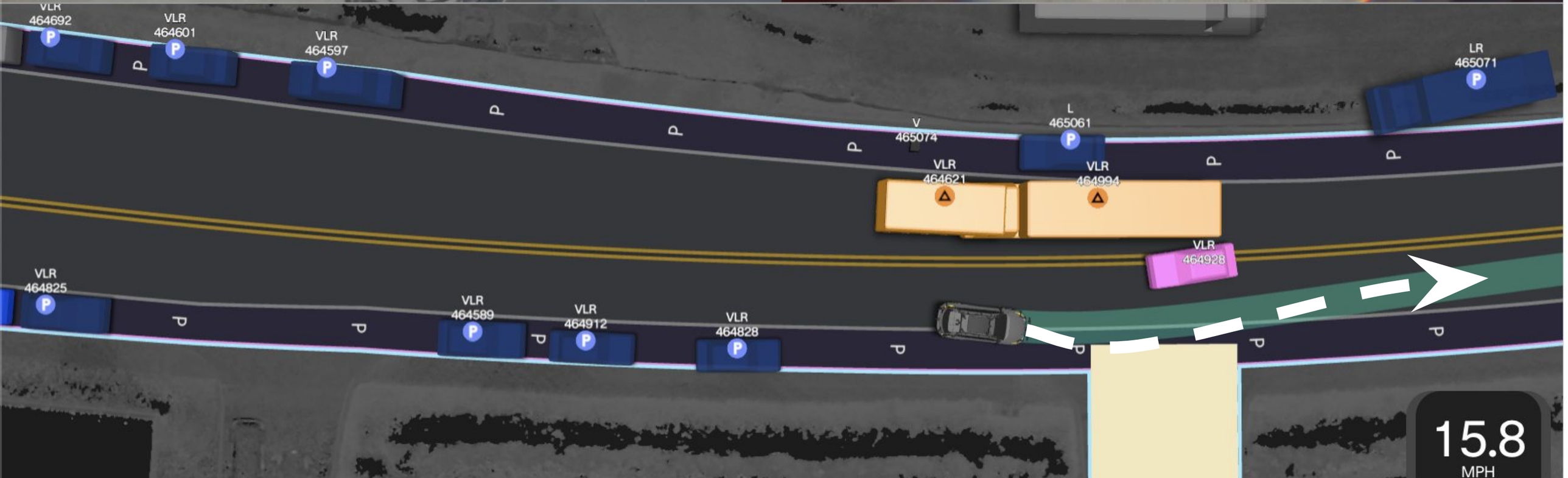


Send command



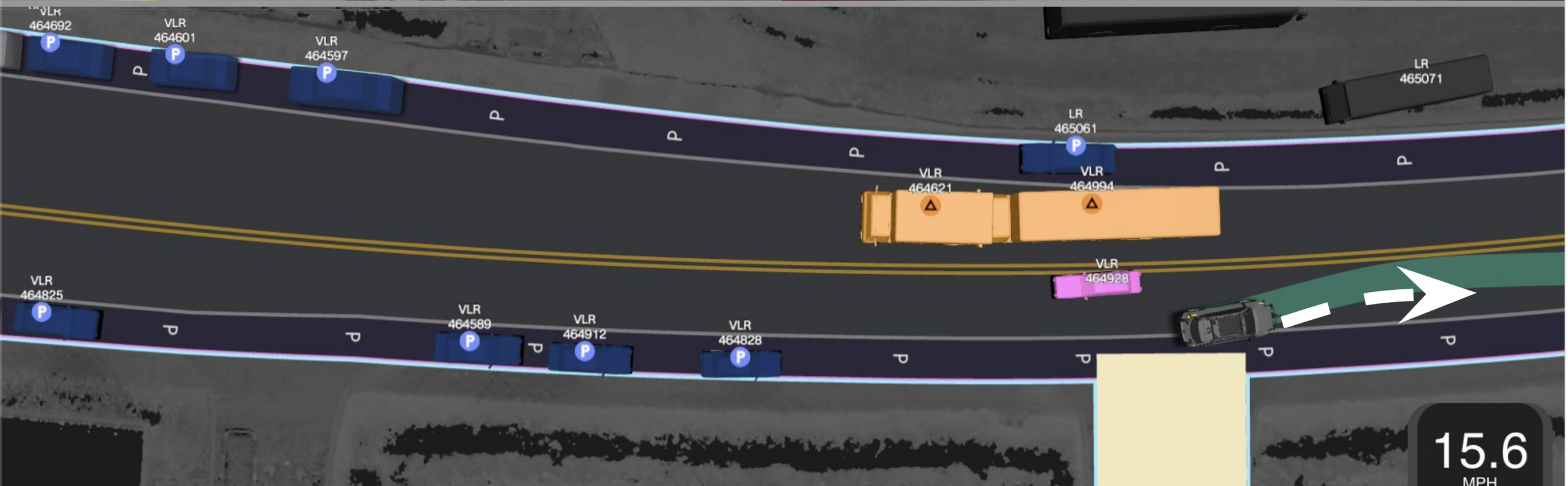
See if it passes





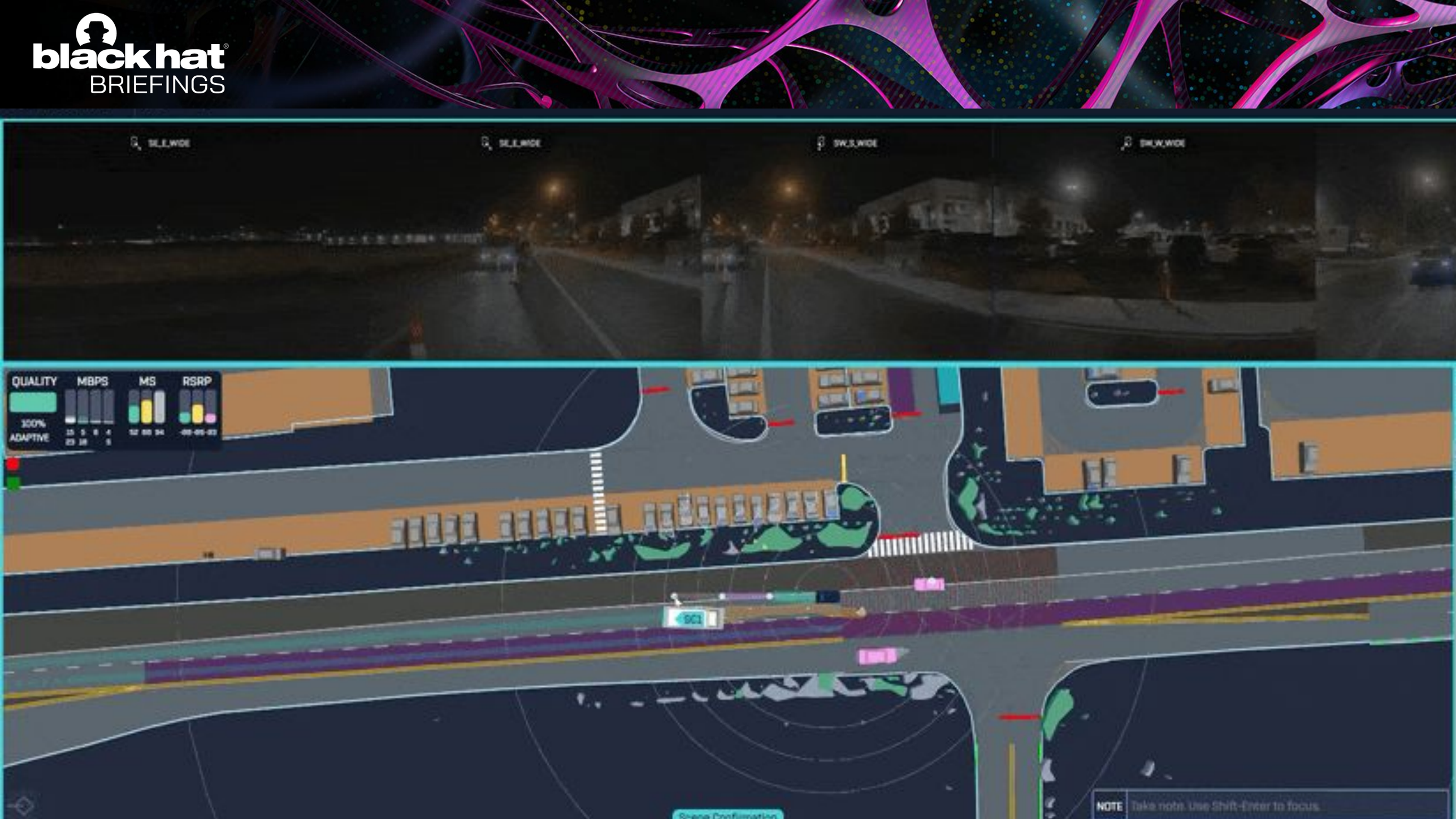
black hat BRIEFINGS

See if it passes



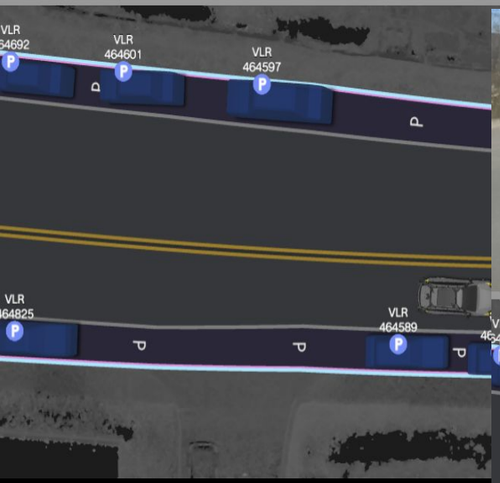
How About Mistakes?

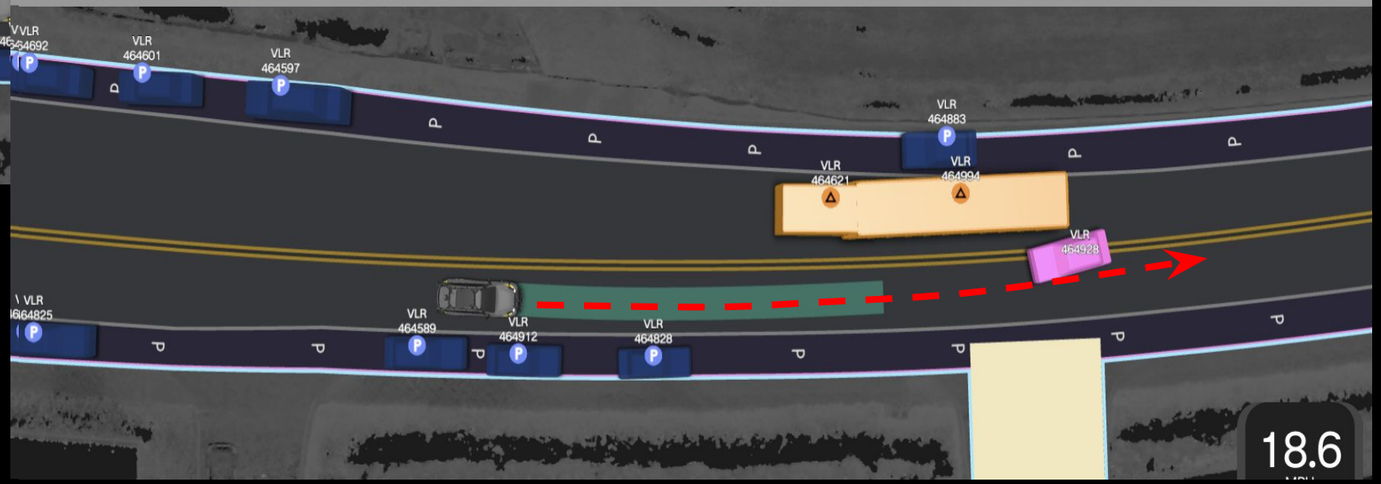

black hat
BRIEFINGS
QUALITY
MBPS
MS
RSRP
100%
ADAPTIVE
15 5 8 4
21 18 3
52 87 94
-87 -65 -93
SC1


black hat
BRIEFINGS
SE_E_WIDE
SE_E_WIDE
SW_S_WIDE
SW_W_WIDE
QUALITY
MBPS
MS
RSRP
100%
ADAPTIVE
NOTE
Take note. Use Shift-Enter to focus.

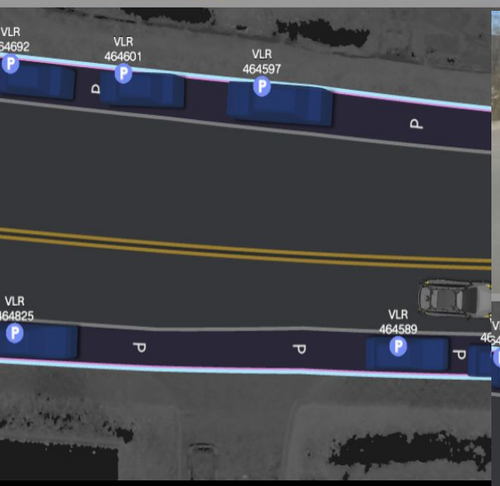

black hat
BRIEFINGS
Engaged
Teleop
SPEED
LIMIT
25
MPH

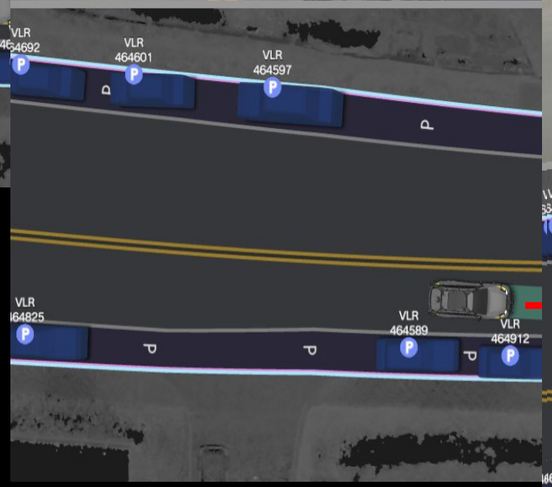
Adversarial variations

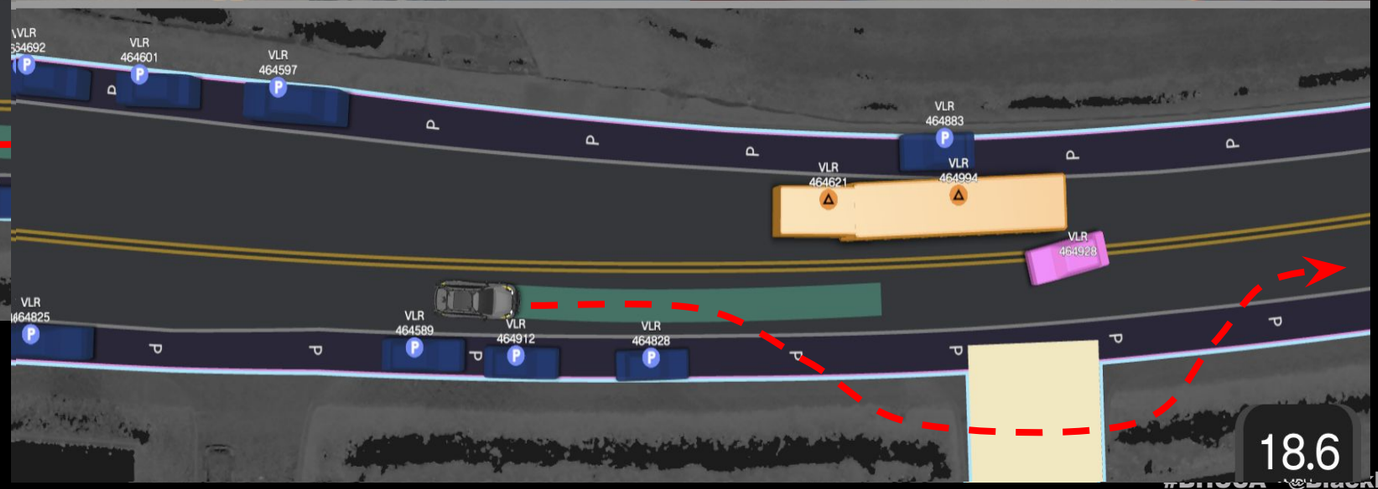


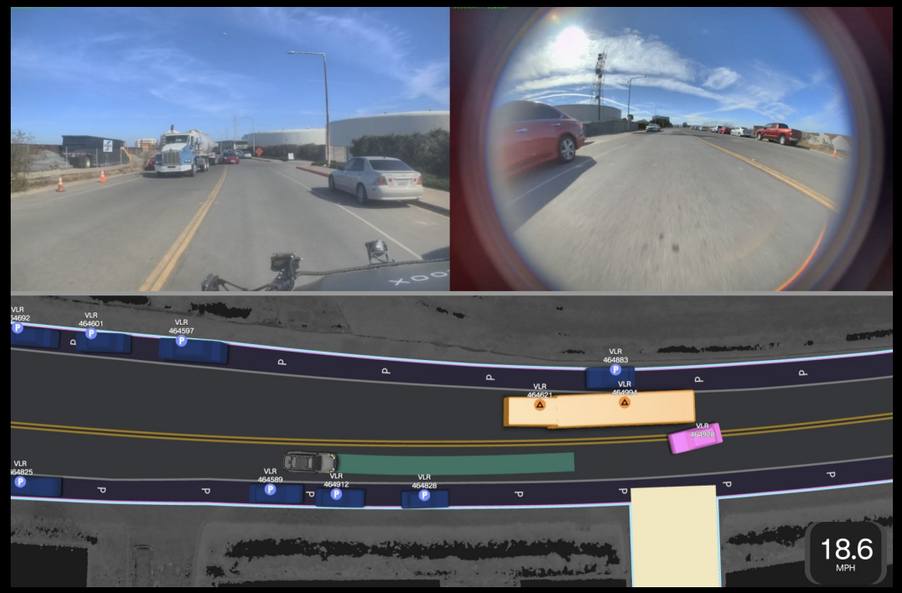


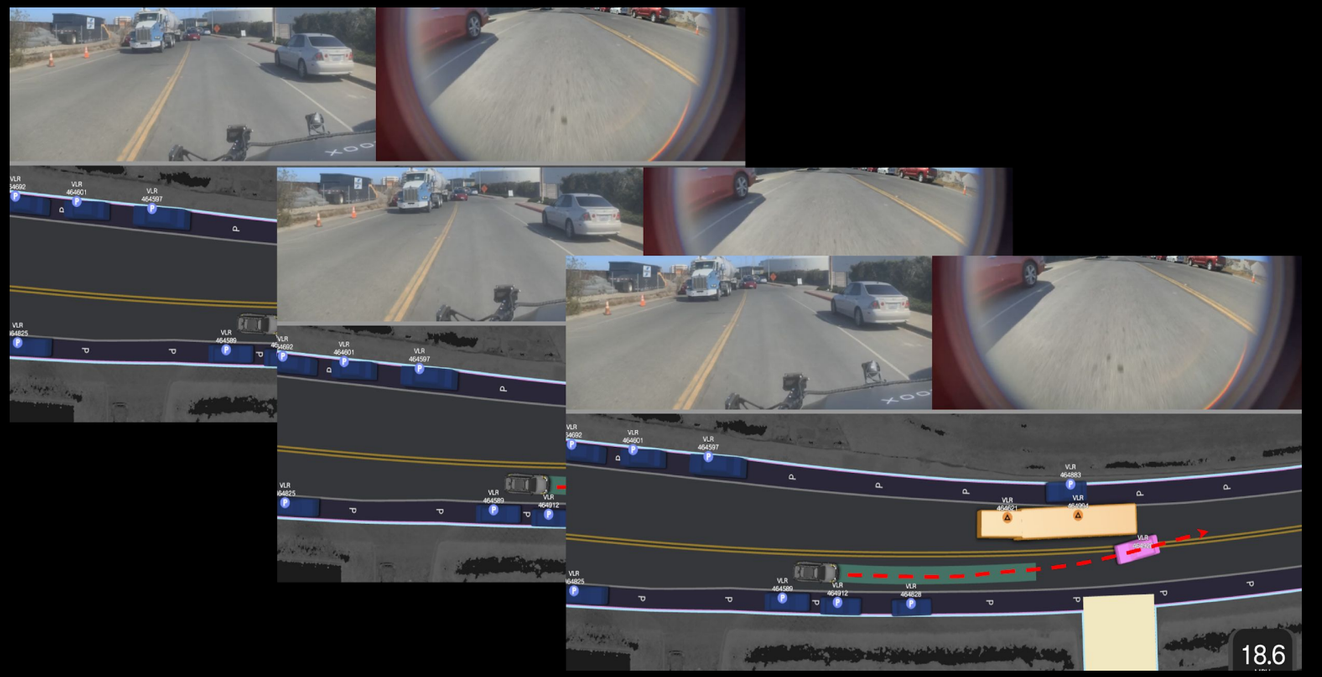
Adversarial variations





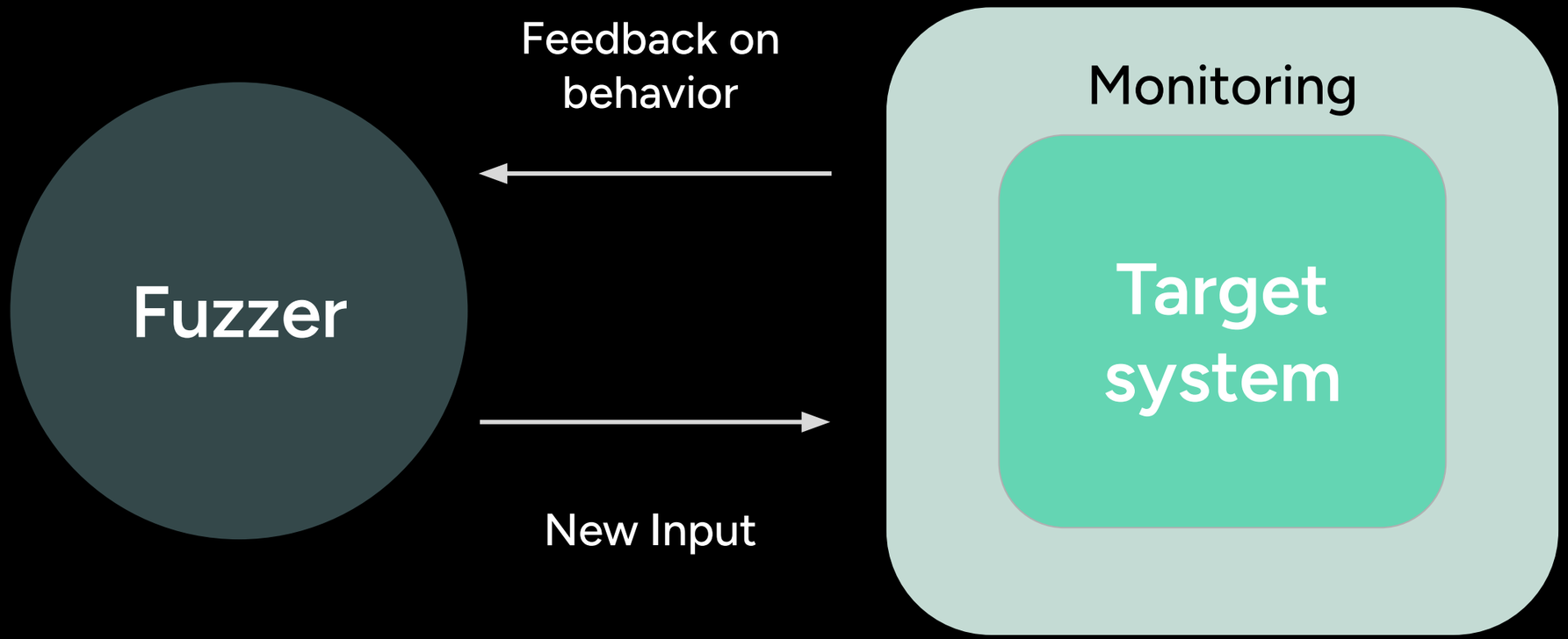


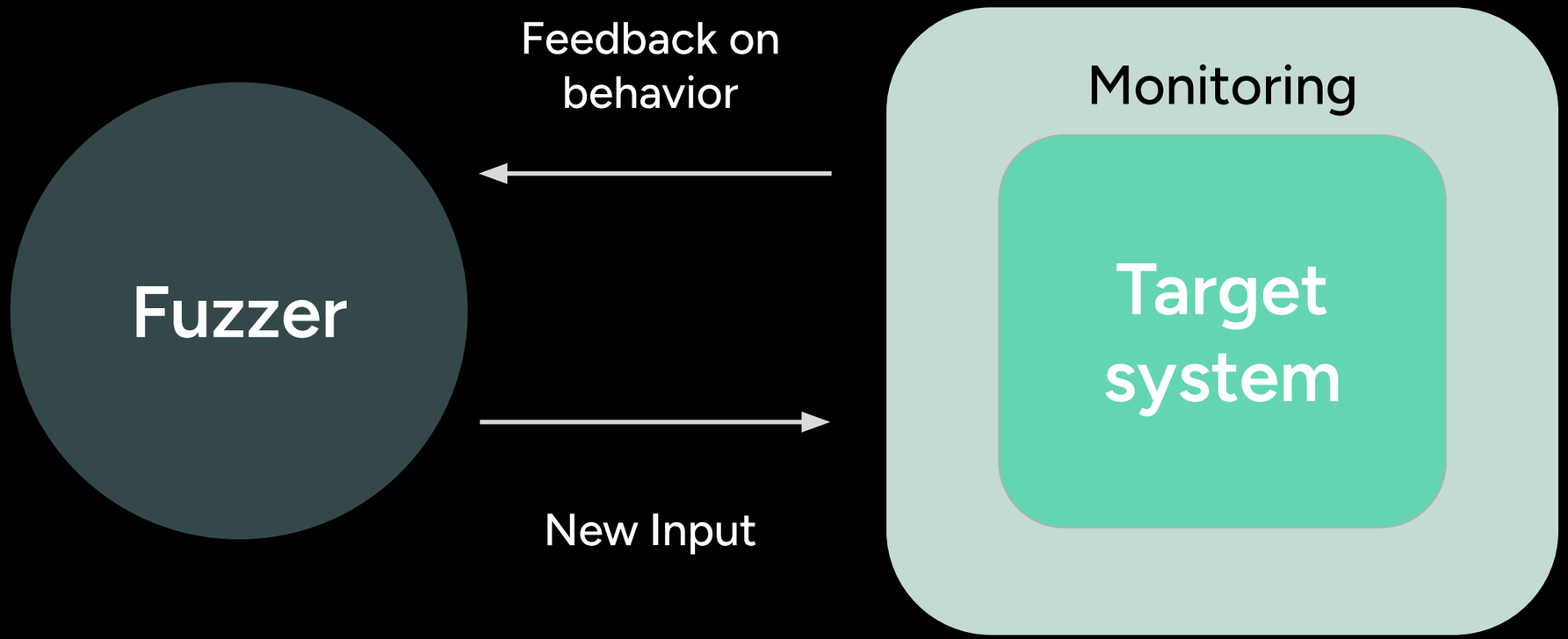

18.6
MPH

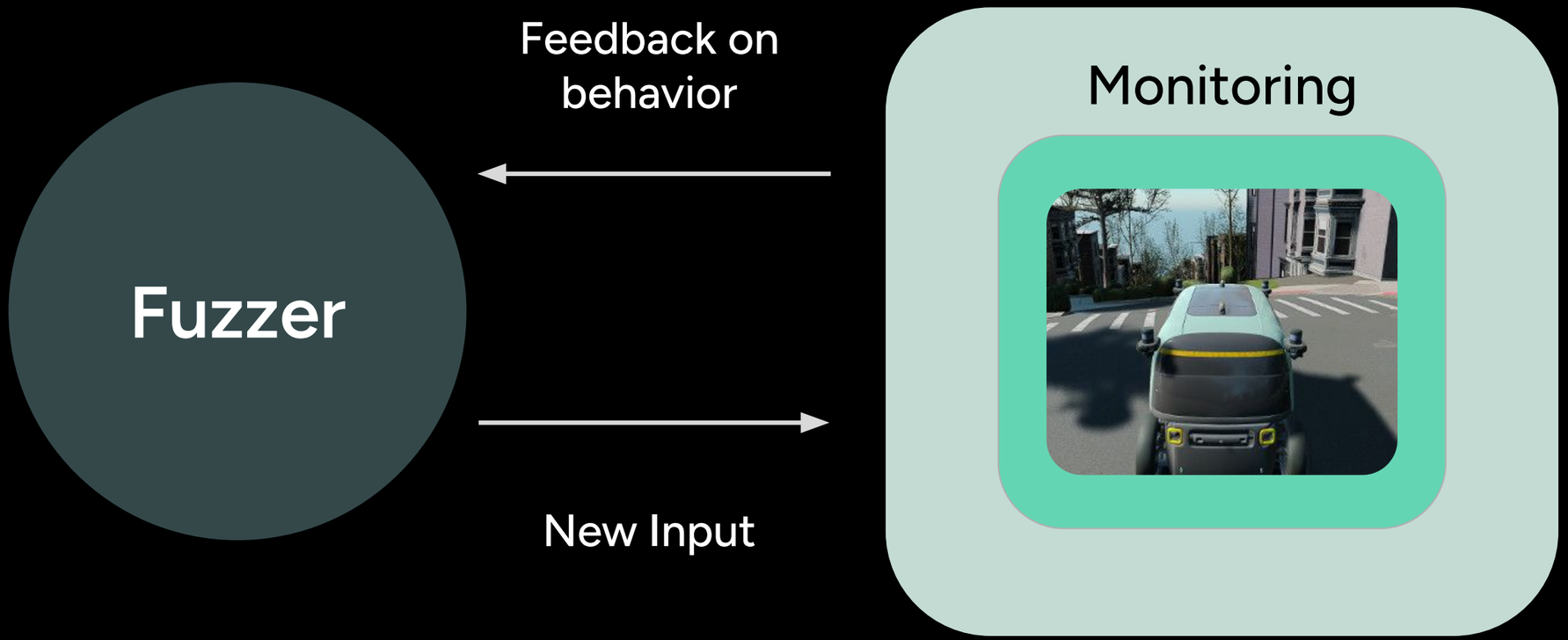

18.6


Show URI
SD
CRIME JUNKIE
SAT MAY 17
18.6
MPH
Show URI
14.6
MPH
5.3
MPH

Is There A Scalable Way?


Feedback on behavior
Fuzzer
Monitoring
Target system
New Input


Feedback on behavior
Fuzzer
Monitoring
Target system
New Input

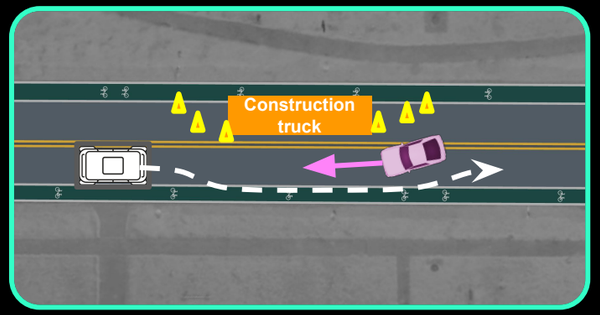

Feedback on behavior
Fuzzer
Monitoring
New Input

Suggested Path
AV
Other Car

Feedback on behavior

Fuzzer

Monitoring

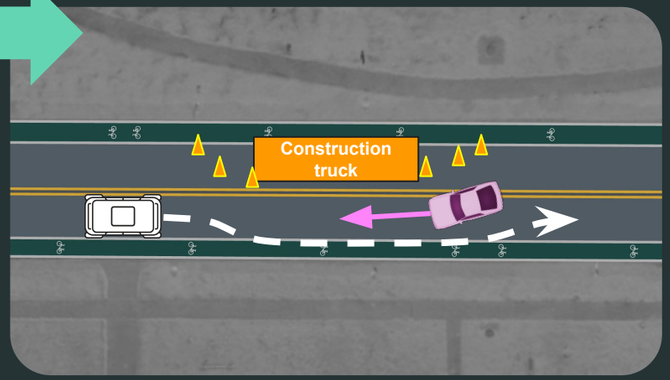


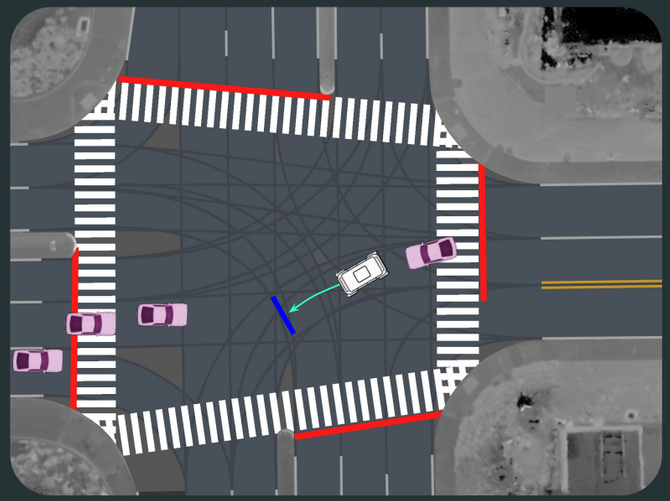
Complex real-world situations

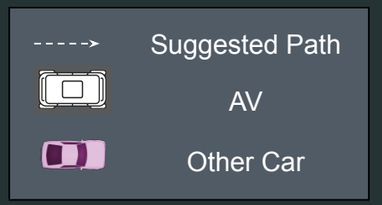
Complex real-world situations

Extract

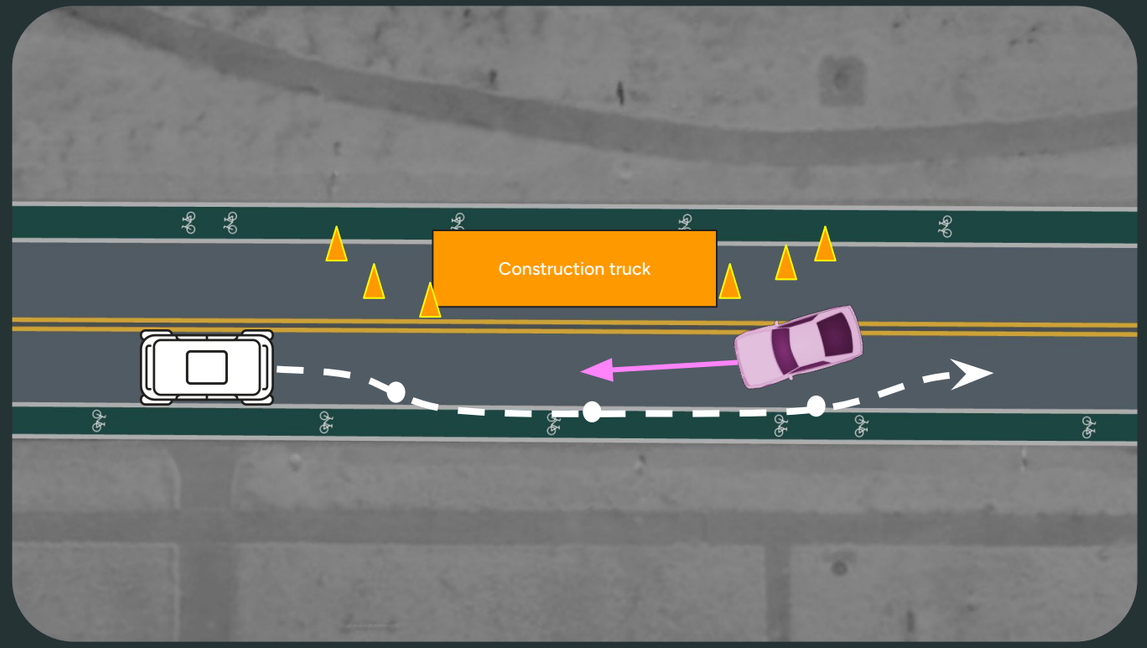
Base scenario







Base Scenario

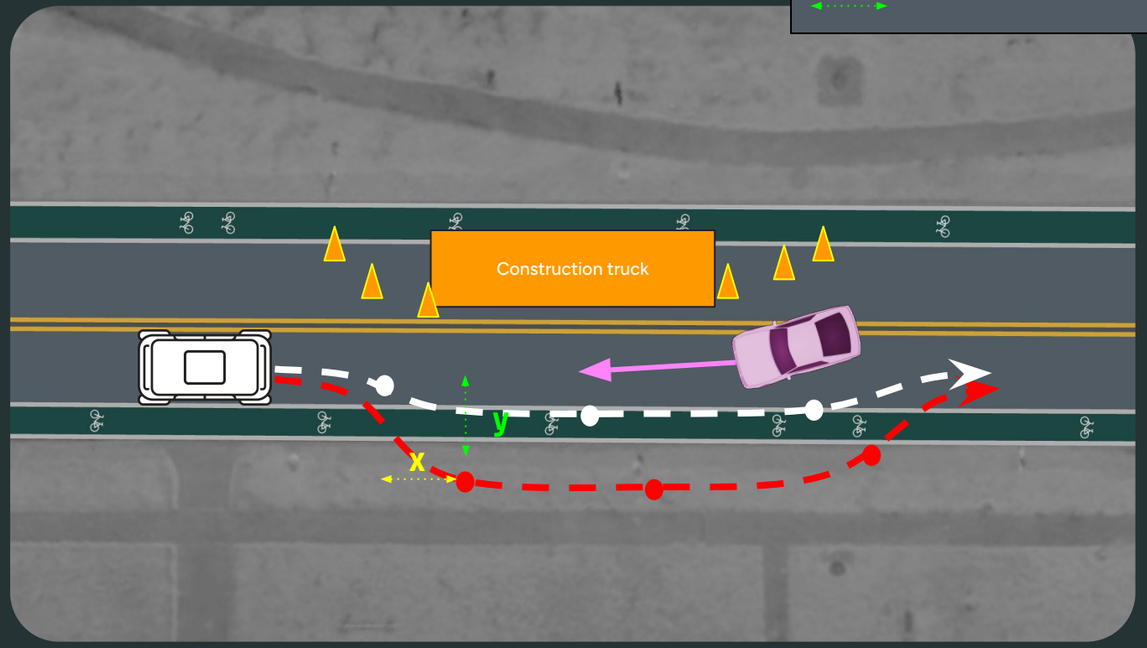


Add TO params

Input

x longitudinal offset

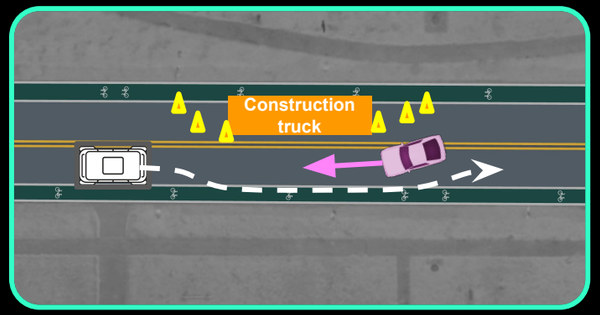
y Lateral offset

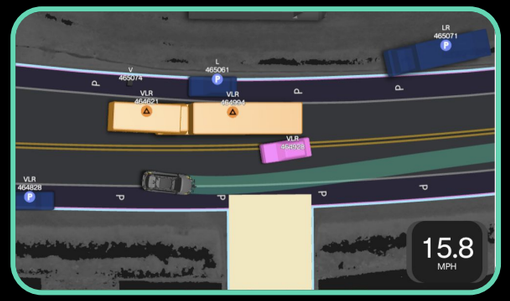


Feedback on behavior

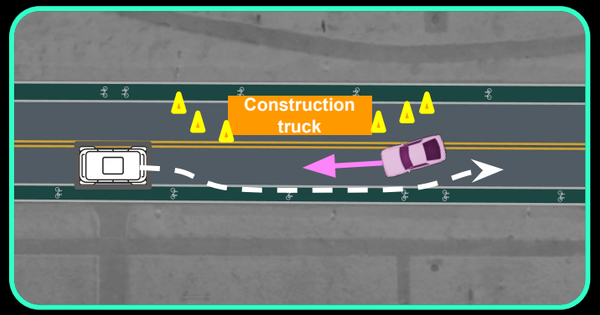
Fuzzer

Monitoring



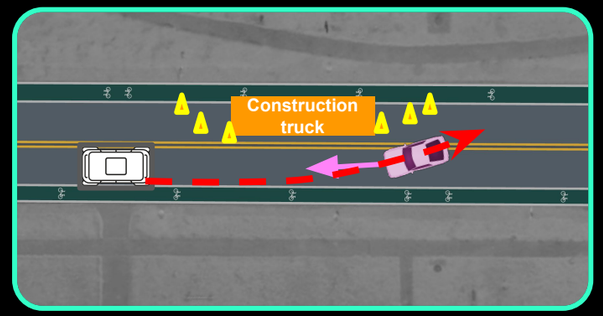


Fuzzer

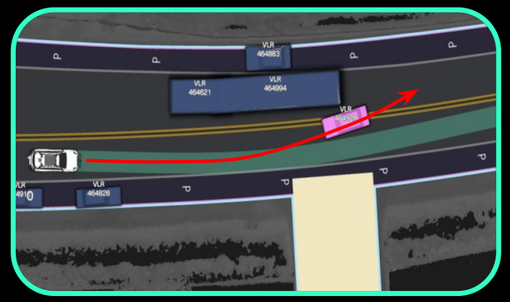


Monitoring

Fuzzer

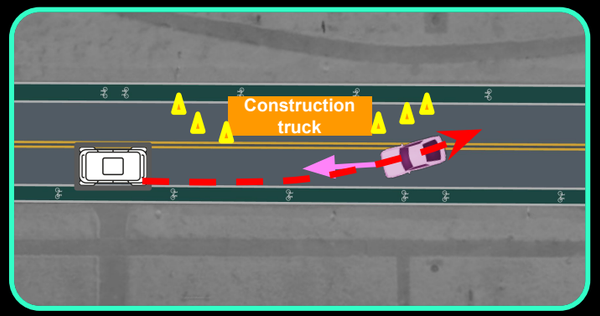


Monitoring



Fuzzer

Monitoring

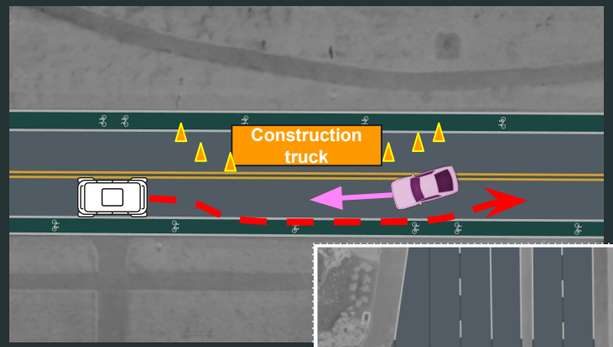


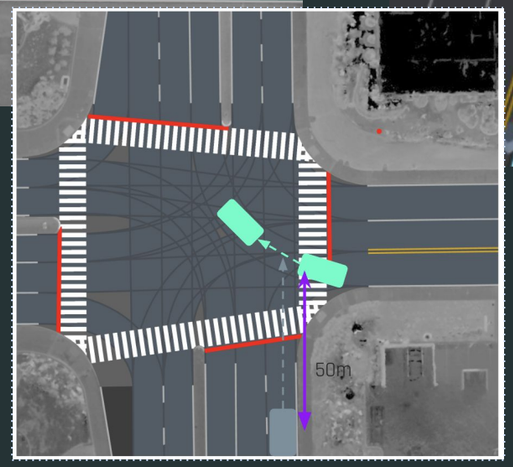
What We Discovered

Some numbers

Base scenarios

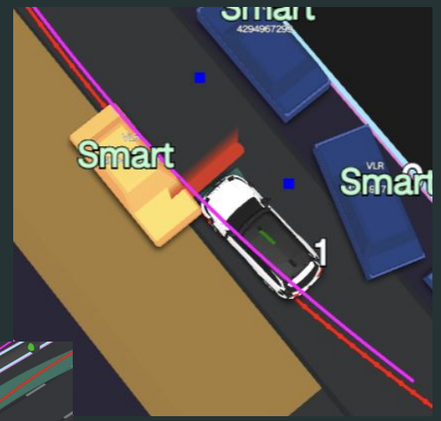
- 300+ situations
- different geometries, type





Variations

- 50,000+ mutants
- 3 valid collisions



Case 1

Merging from Parking

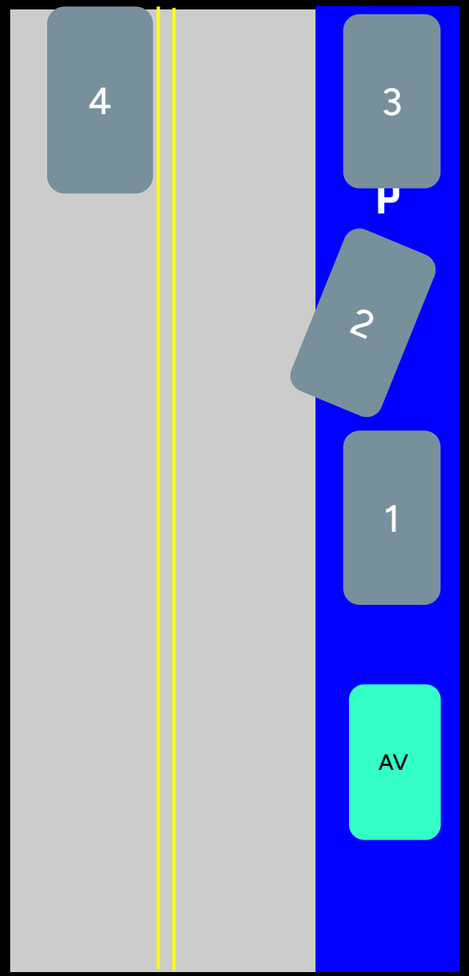
Case 2

Reversing into Intersection

Case 3

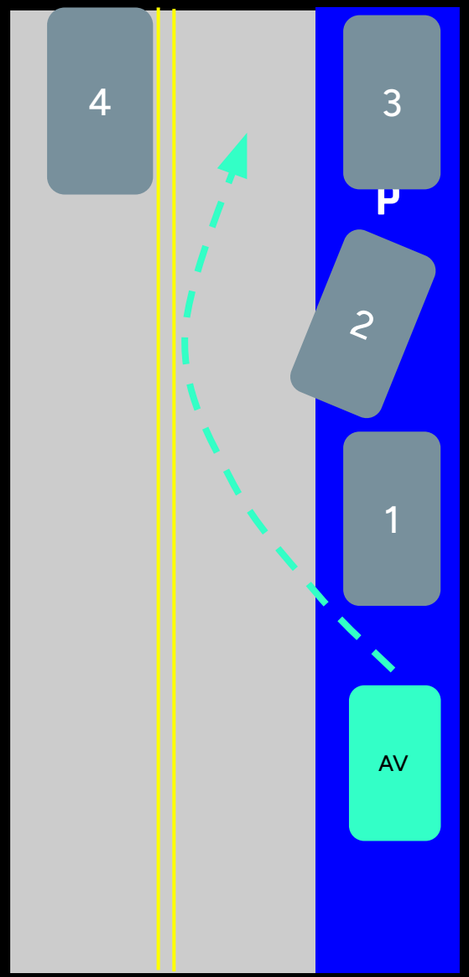
Right Turn with Multi-Agent Interaction

Case 1: Merging from Parking



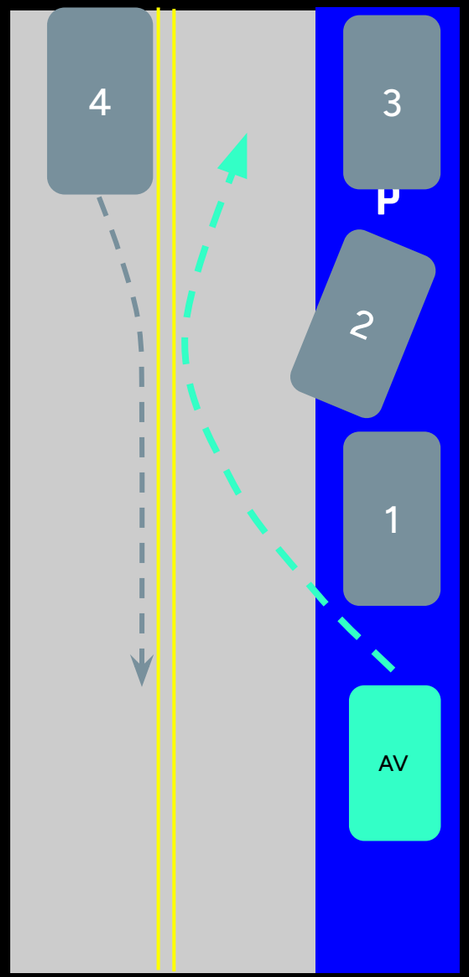
Situation type	Get on road from parking spot

Case 1: Merging from Parking



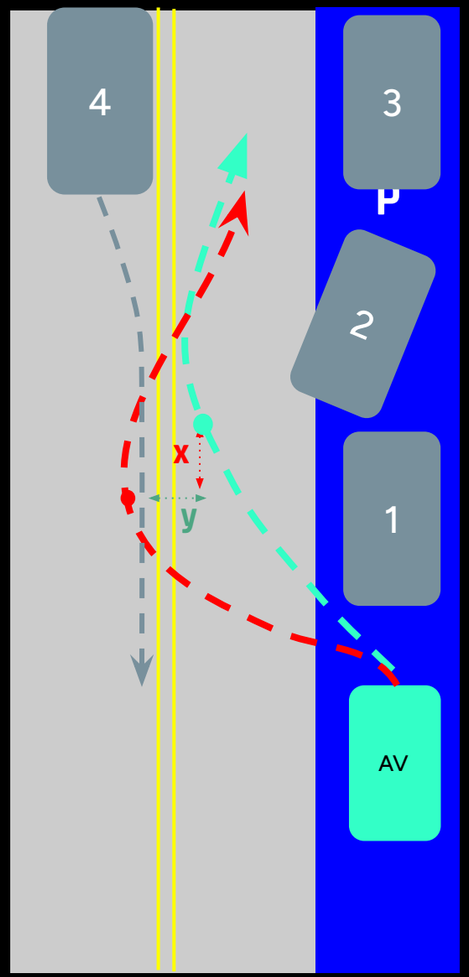
Situation type	Get on road from parking spot
AV maneuver	AV stopped in parking lane, following suggested waypoints to get on road

Case 1: Merging from Parking

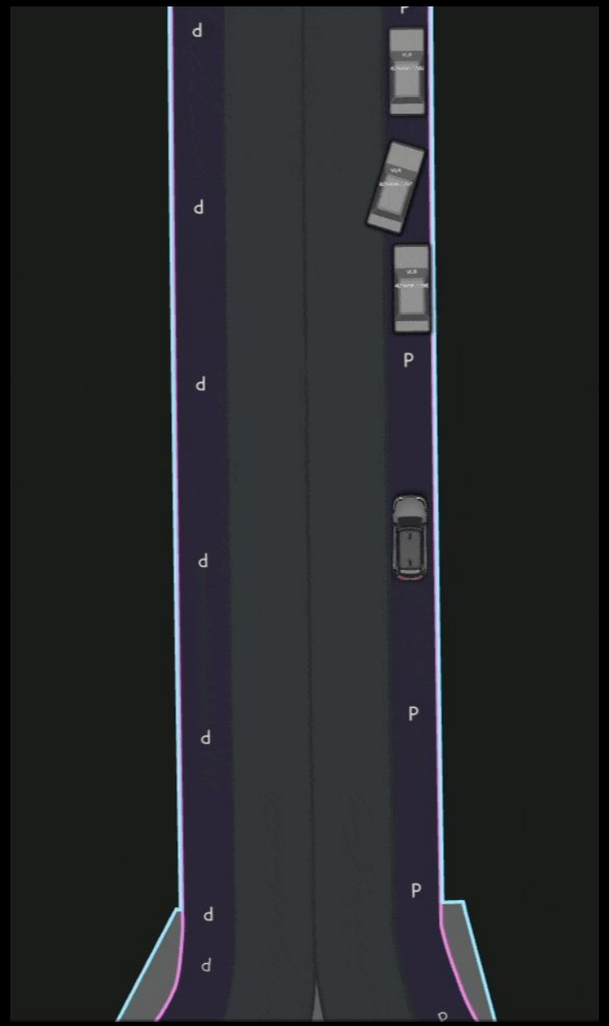


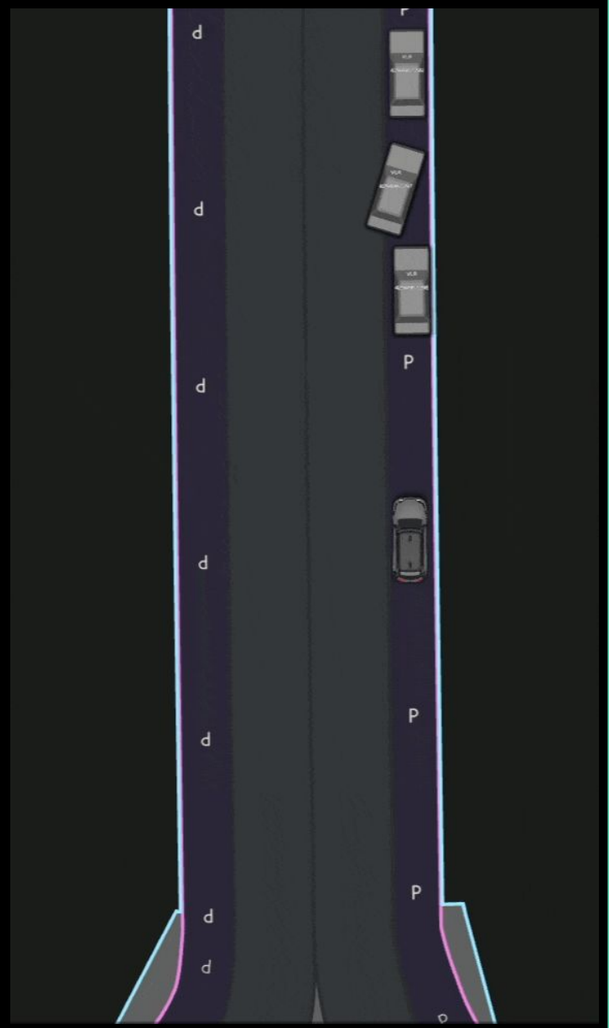
Situation type	Get on road from parking spot
AV maneuver	AV stopped in parking lane, following suggested waypoints to get on road
Agent maneuver	[Agent 1-3] ahead of AV, stopped [Agent 4] ahead of AV, driving following the route

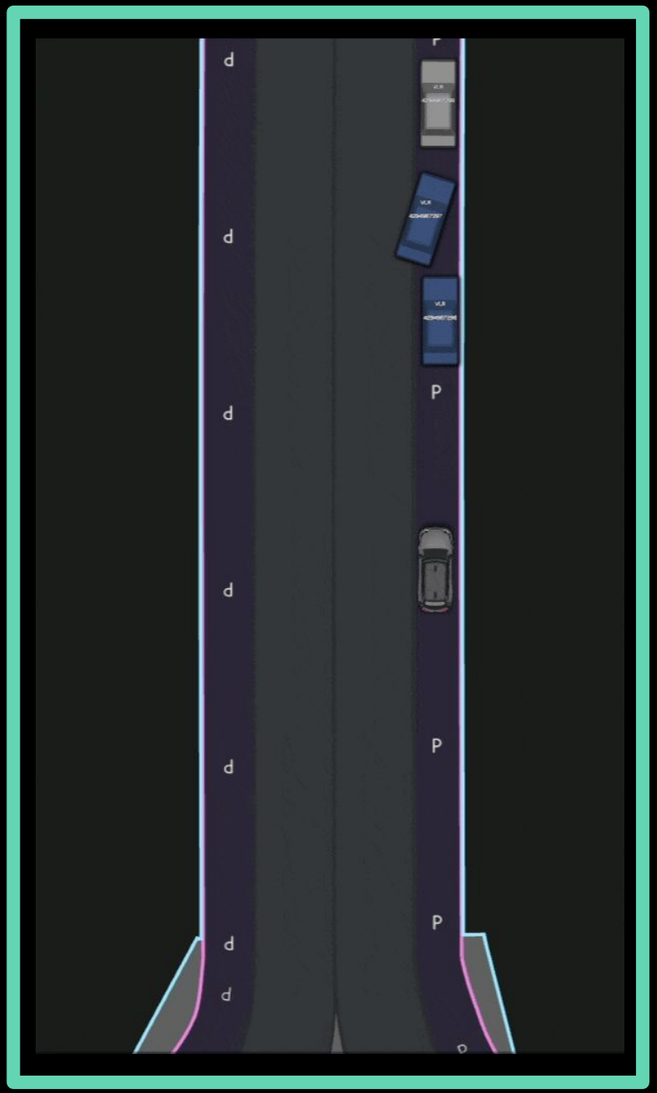
Case 1: Merging from Parking

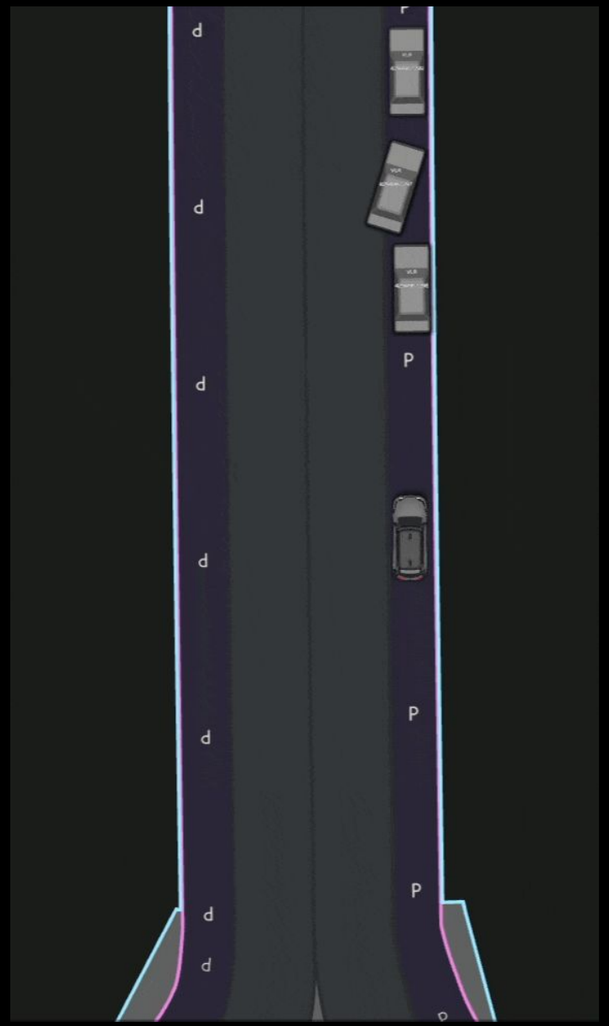


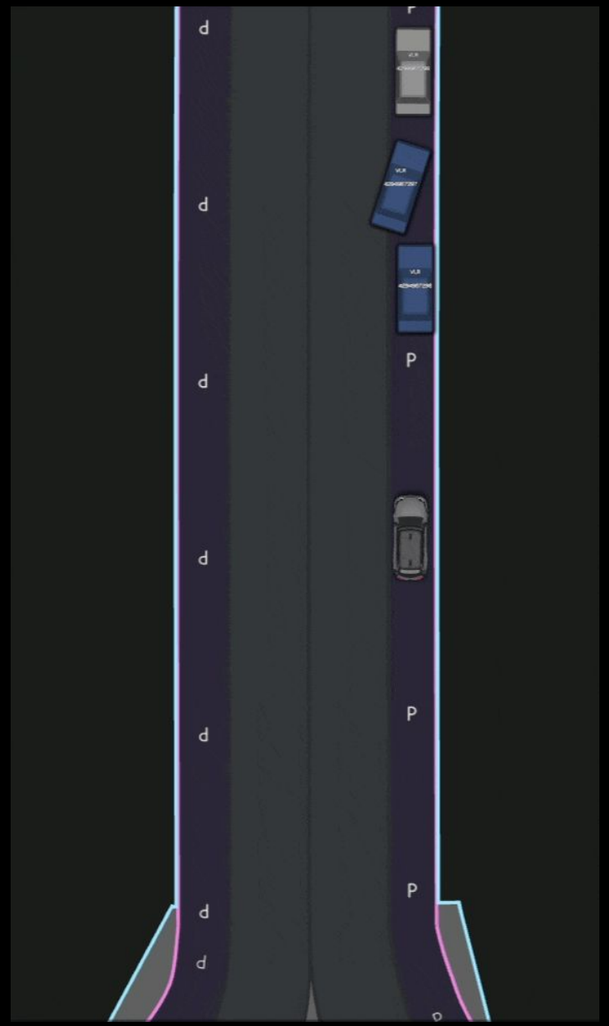
Situation type	Get on road from parking spot
AV maneuver	AV stopped in parking lane, following suggested waypoints to get on road
Agent maneuver	[Agent 1-3] ahead of AV, stopped [Agent 4] ahead of AV, driving following the route
Command variants	Suggested waypoints with new parameters • Longitudinal offset (x) • Lateral offset (y)

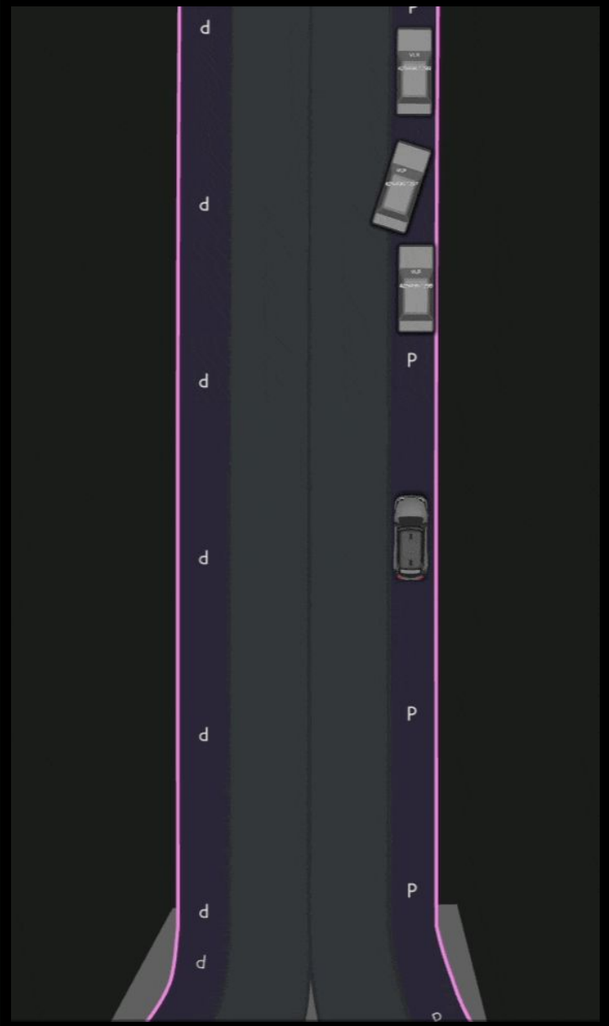

d
d
d
d
d
d
d
P
P
P

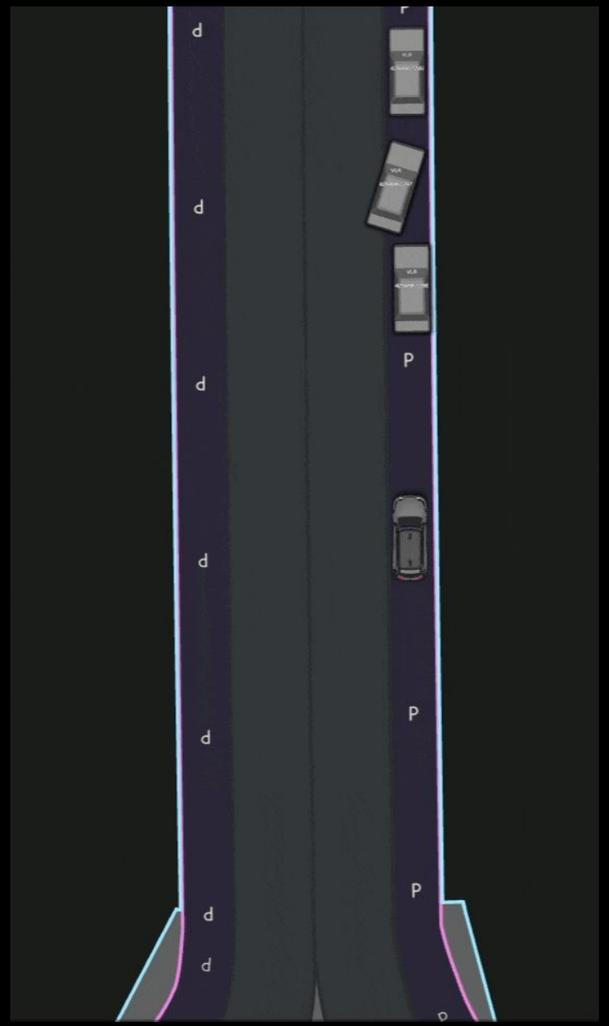

d
d
d
d
d
d
P
P
P

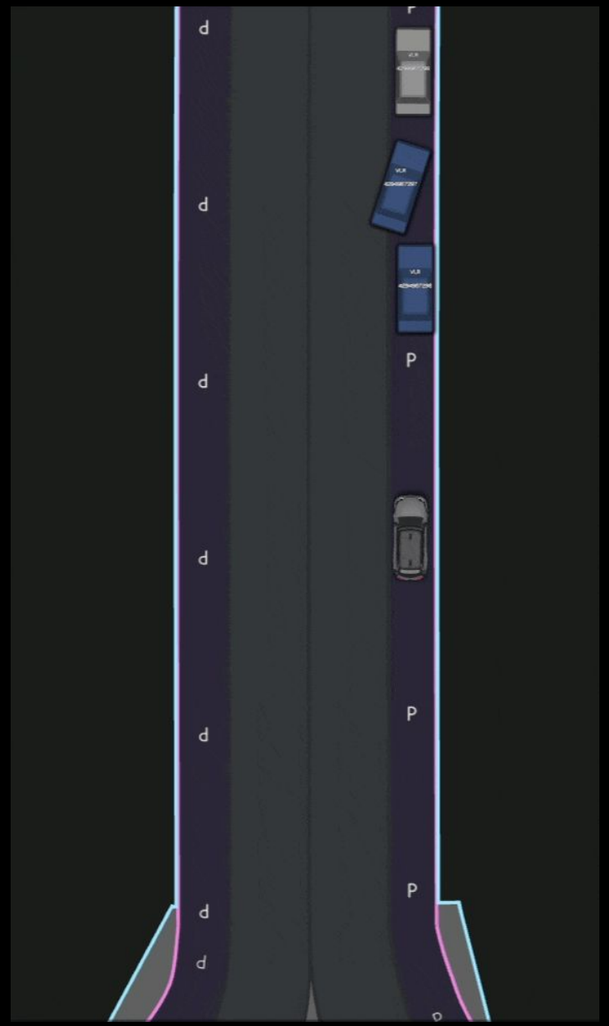

d
d
d
d
d
d
P
P
P

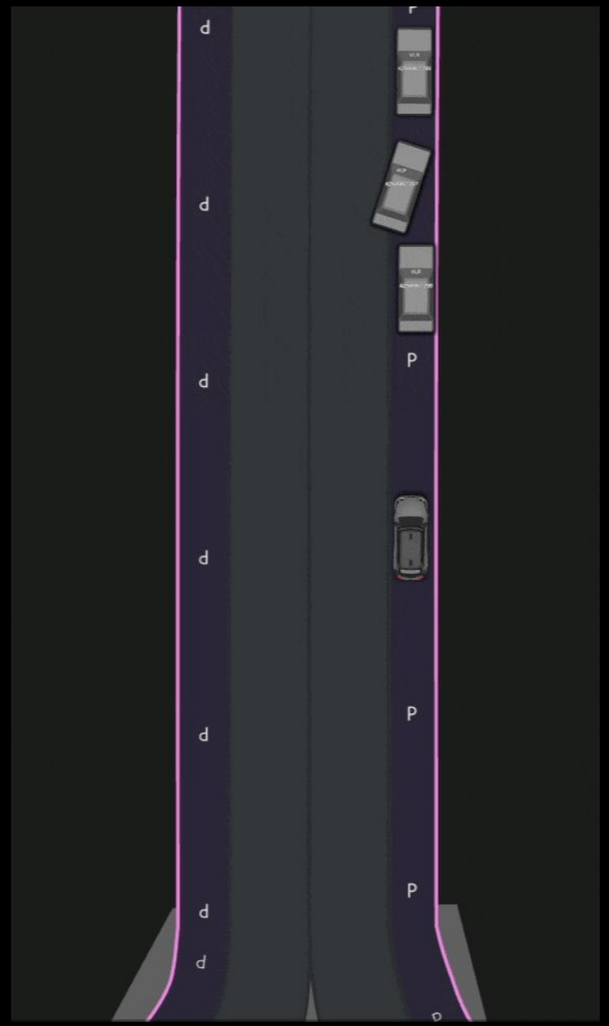

d
d
d
d
d
P
P
P

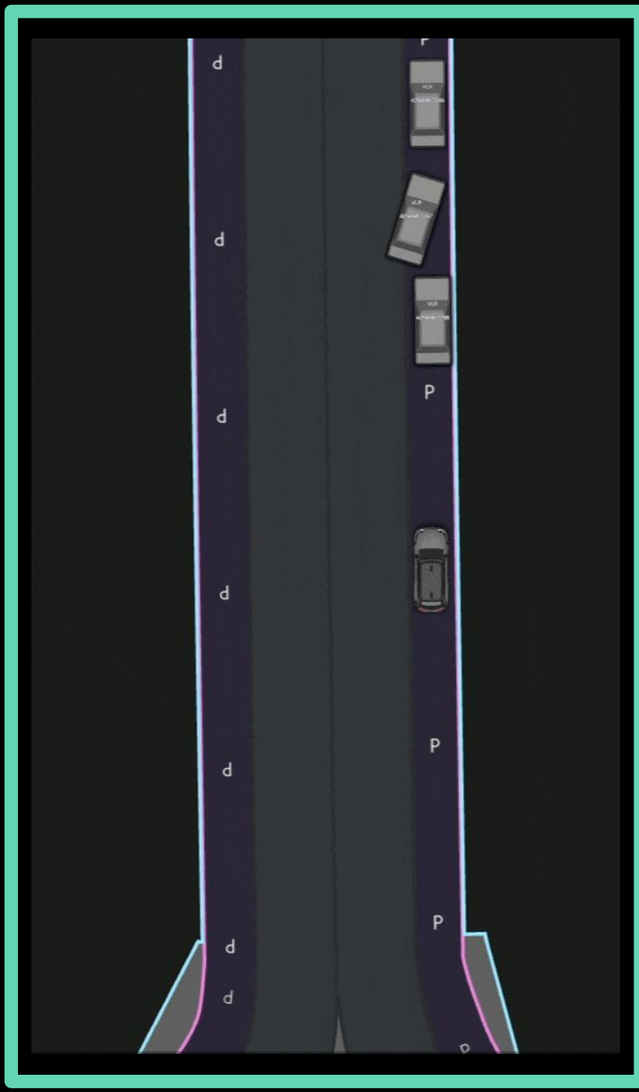

d
d
d
d
d
P
P
P


d
d
d
d
d
P
P
P









Case 1

Merging from Parking

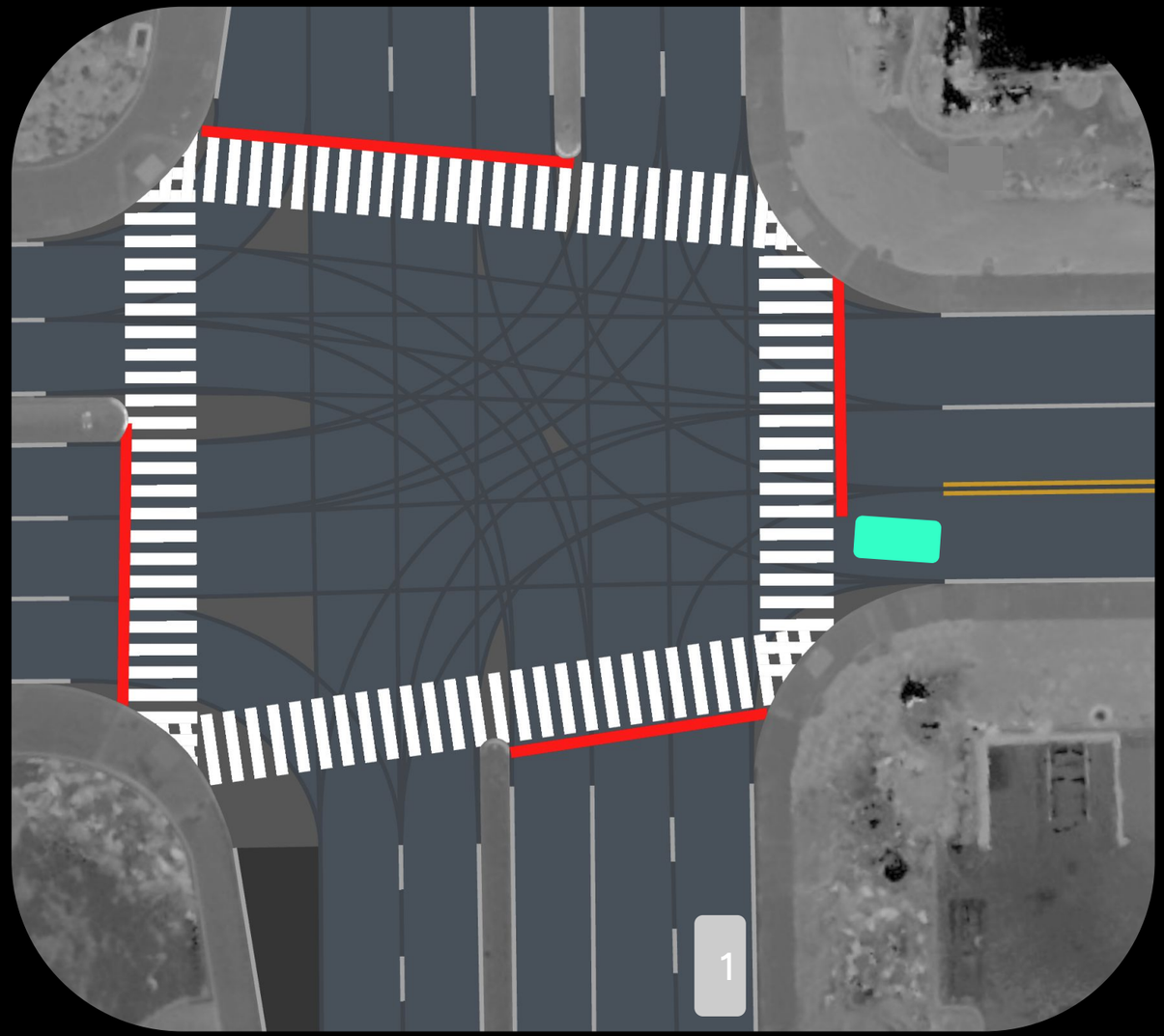
Case 2

Reversing into Intersection

Case 3

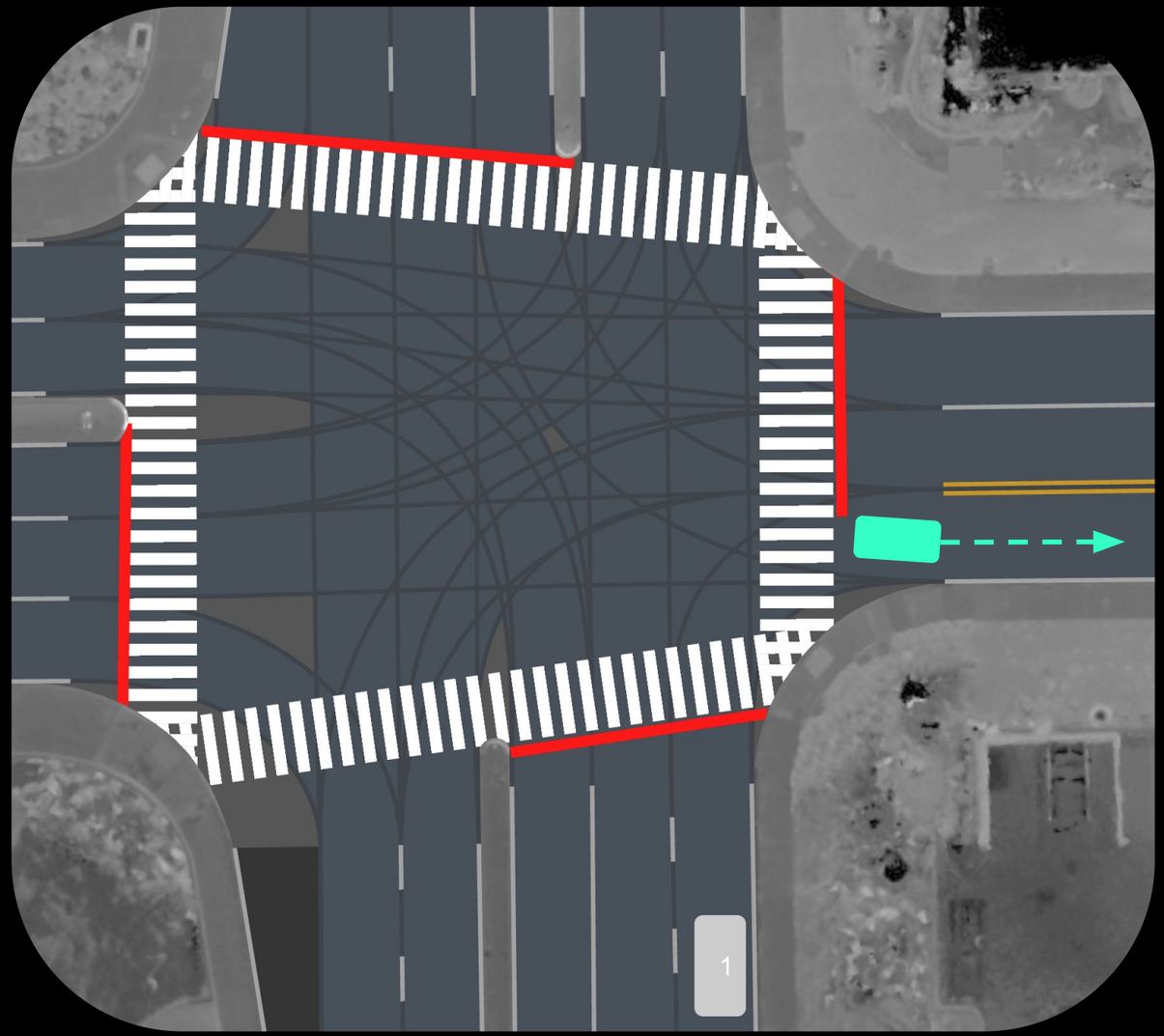
Right Turn with Multi-Agent Interaction

Case 2: Reversing in Intersection



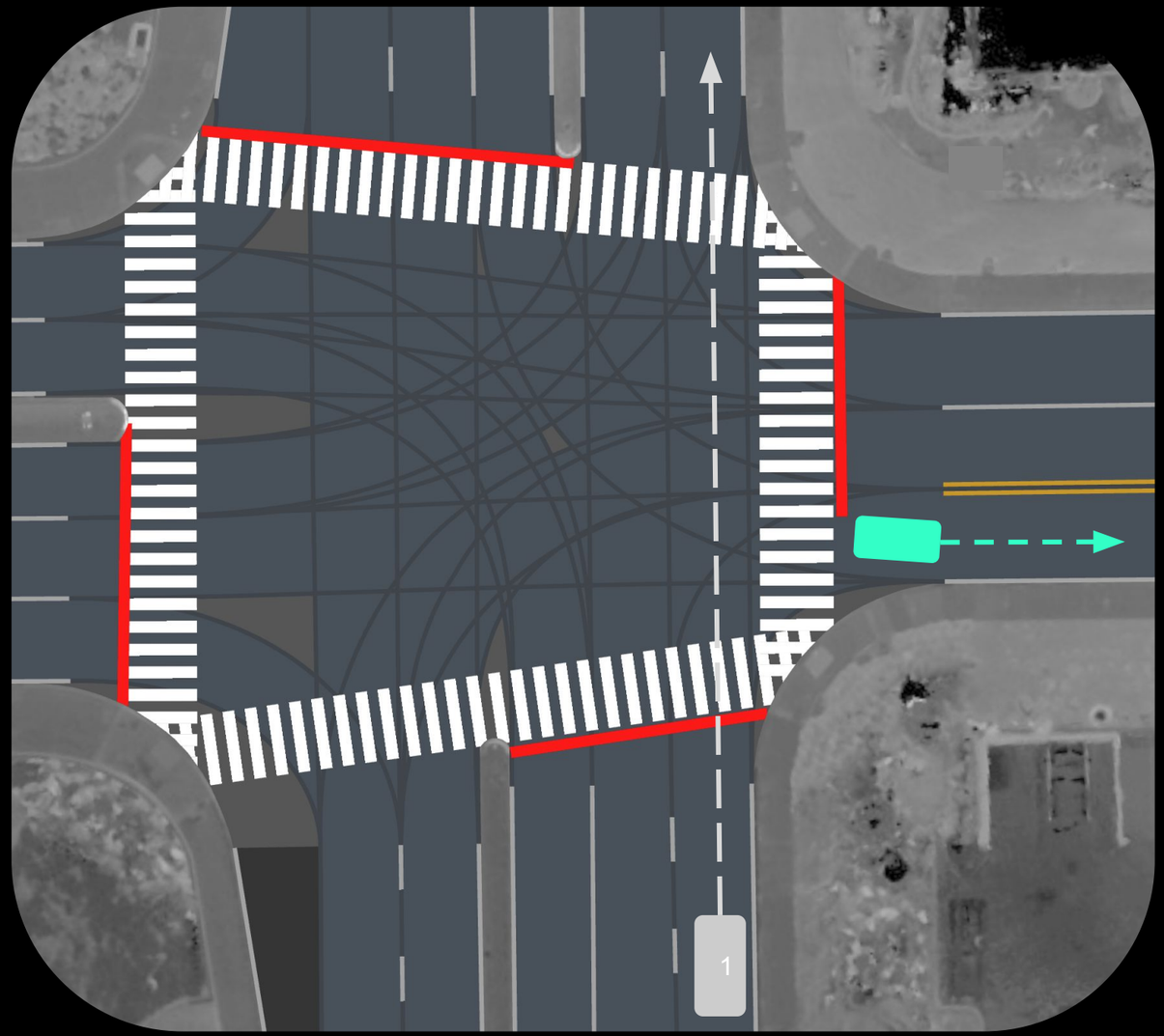
Situation type	Reversing in Intersection

Case 2: Reversing in Intersection



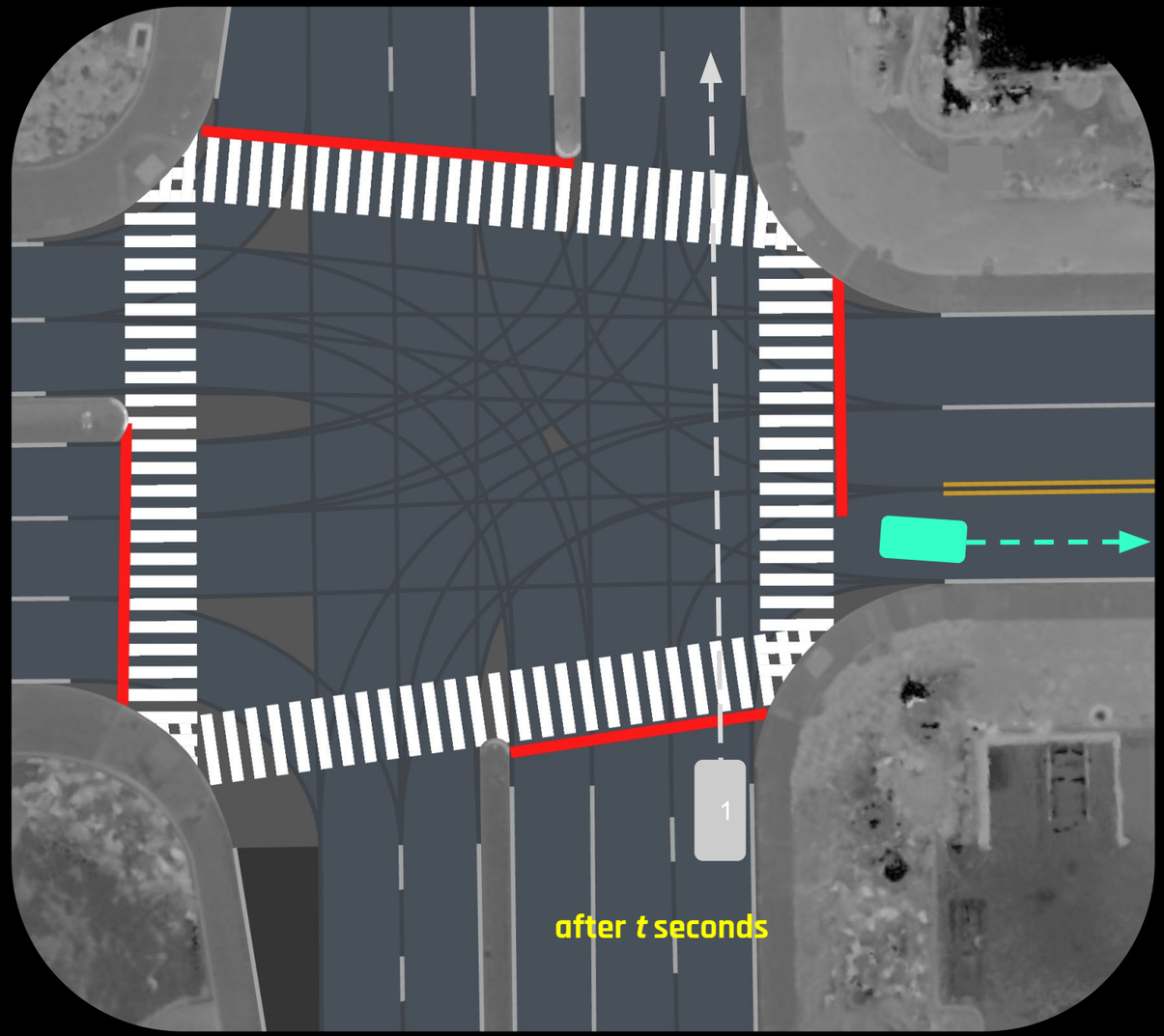
Situation type	Reversing in Intersection
AV maneuver	AV was driving forward away from the intersection

Case 2: Reversing in Intersection



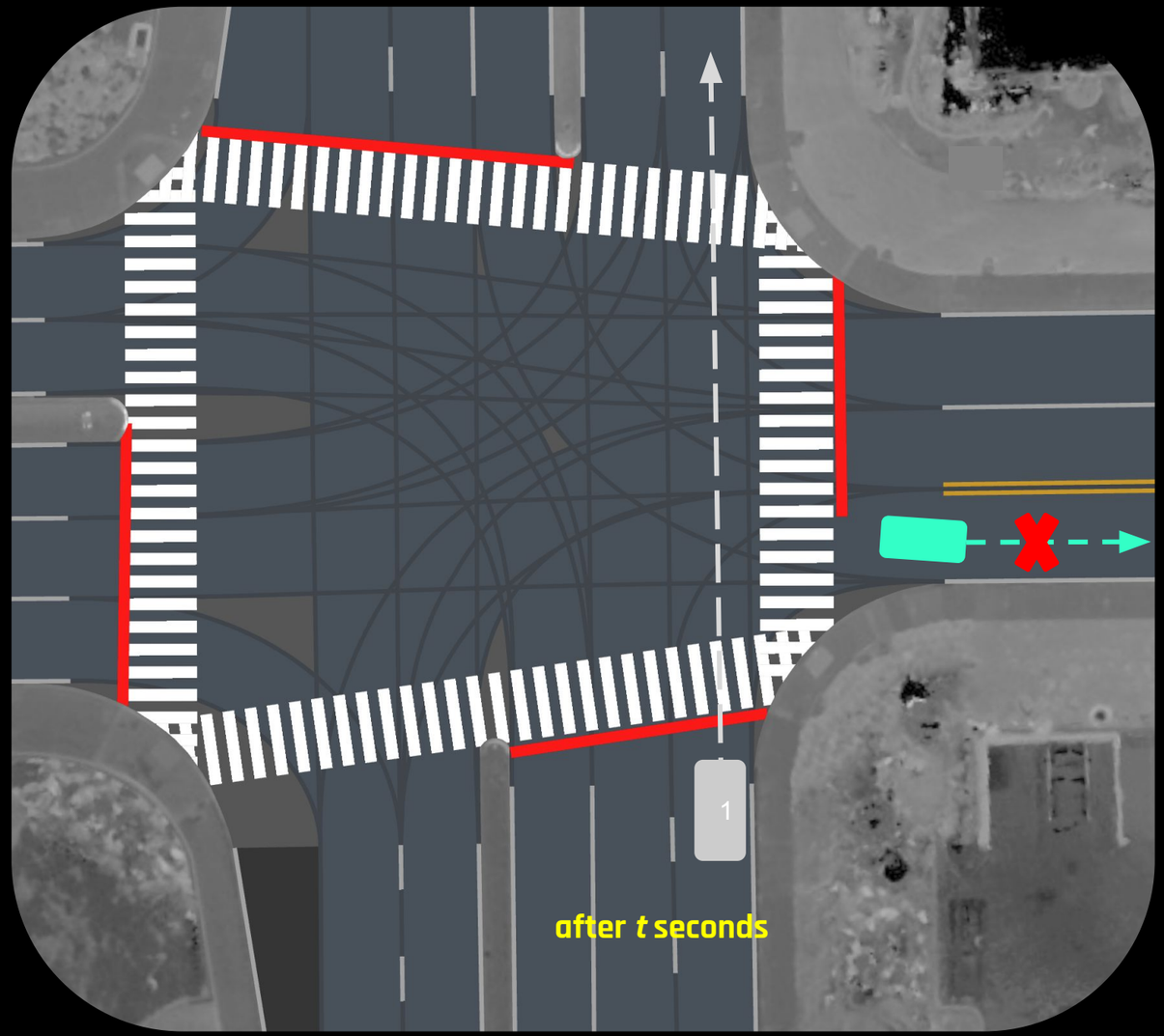
Situation type	Reversing in Intersection
AV maneuver	AV was driving forward away from the intersection
Agent maneuver	[Agent 1] behind AV, crossing intersection with the route

Case 2: Reversing in Intersection



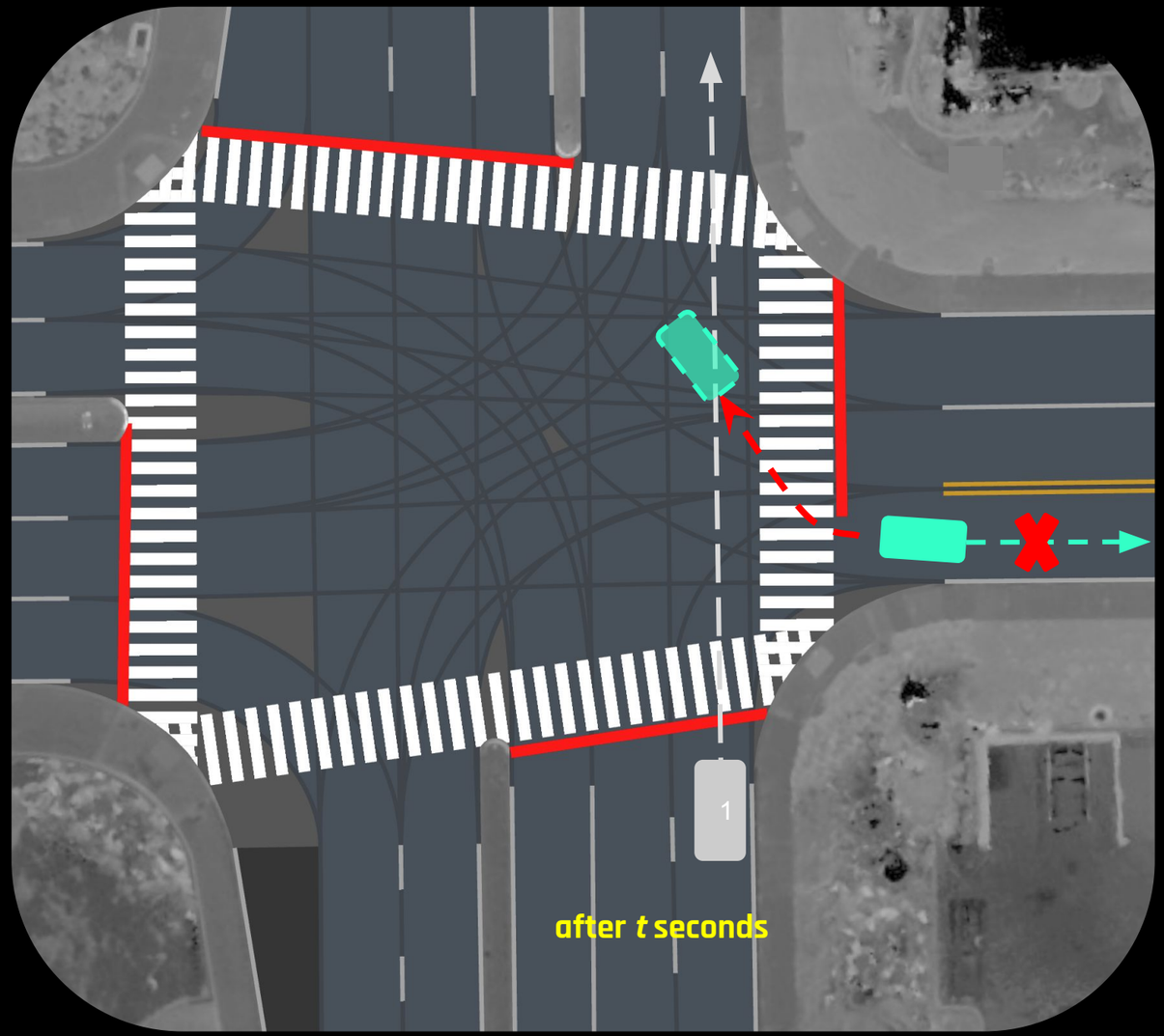
Situation type	Reversing in Intersection
AV maneuver	AV was driving forward away from the intersection
Agent maneuver	[Agent 1] behind AV, crossing intersection with the route
Command variants	Suggested reverse waypoint with new parameters • Start reversing timing (t)

Case 2: Reversing in Intersection



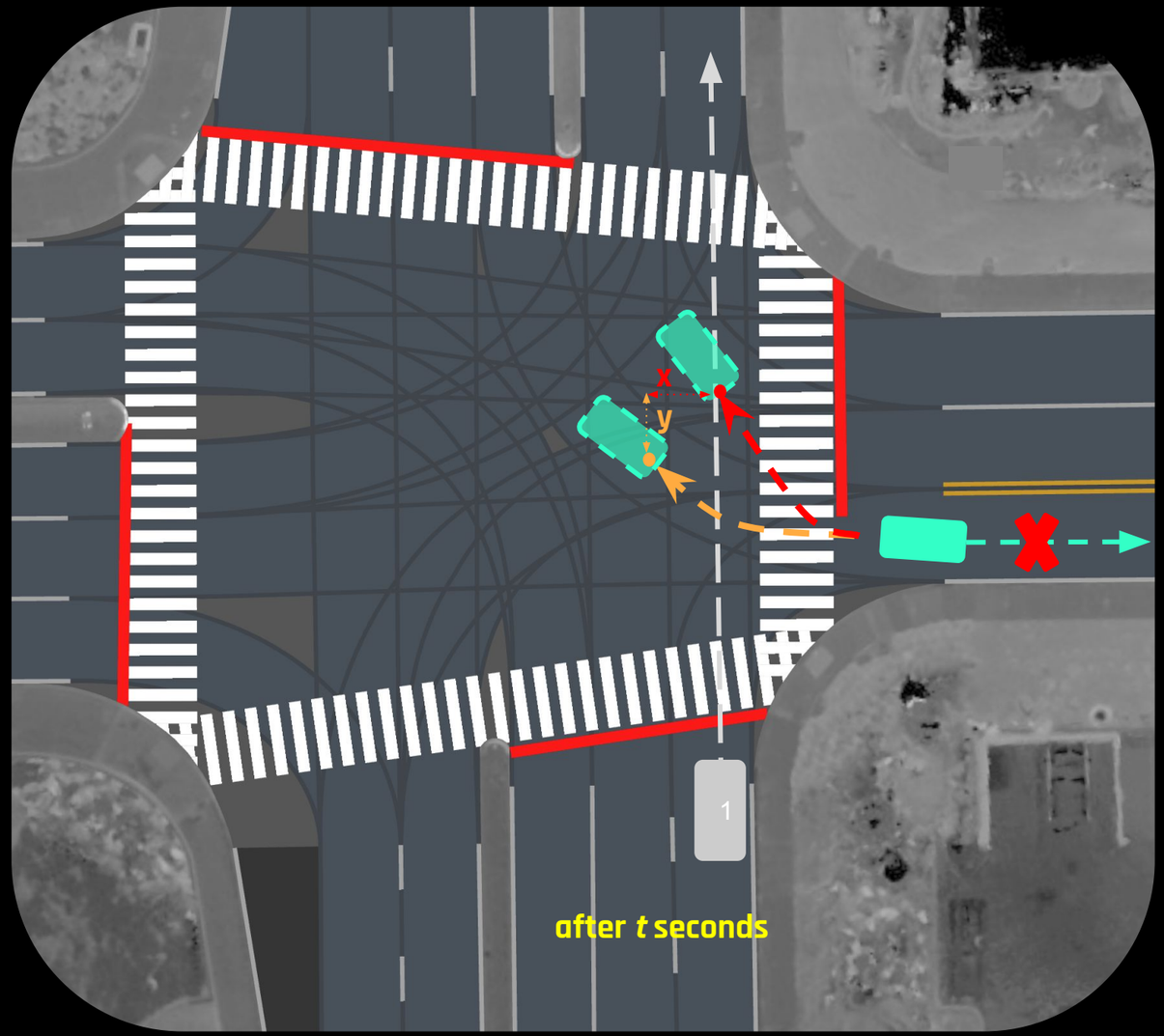
Situation type	Reversing in Intersection
AV maneuver	AV was driving forward away from the intersection
Agent maneuver	[Agent 1] behind AV, crossing intersection with the route
Command variants	Suggested reverse waypoint with new parameters • Start reversing timing (t)

Case 2: Reversing in Intersection

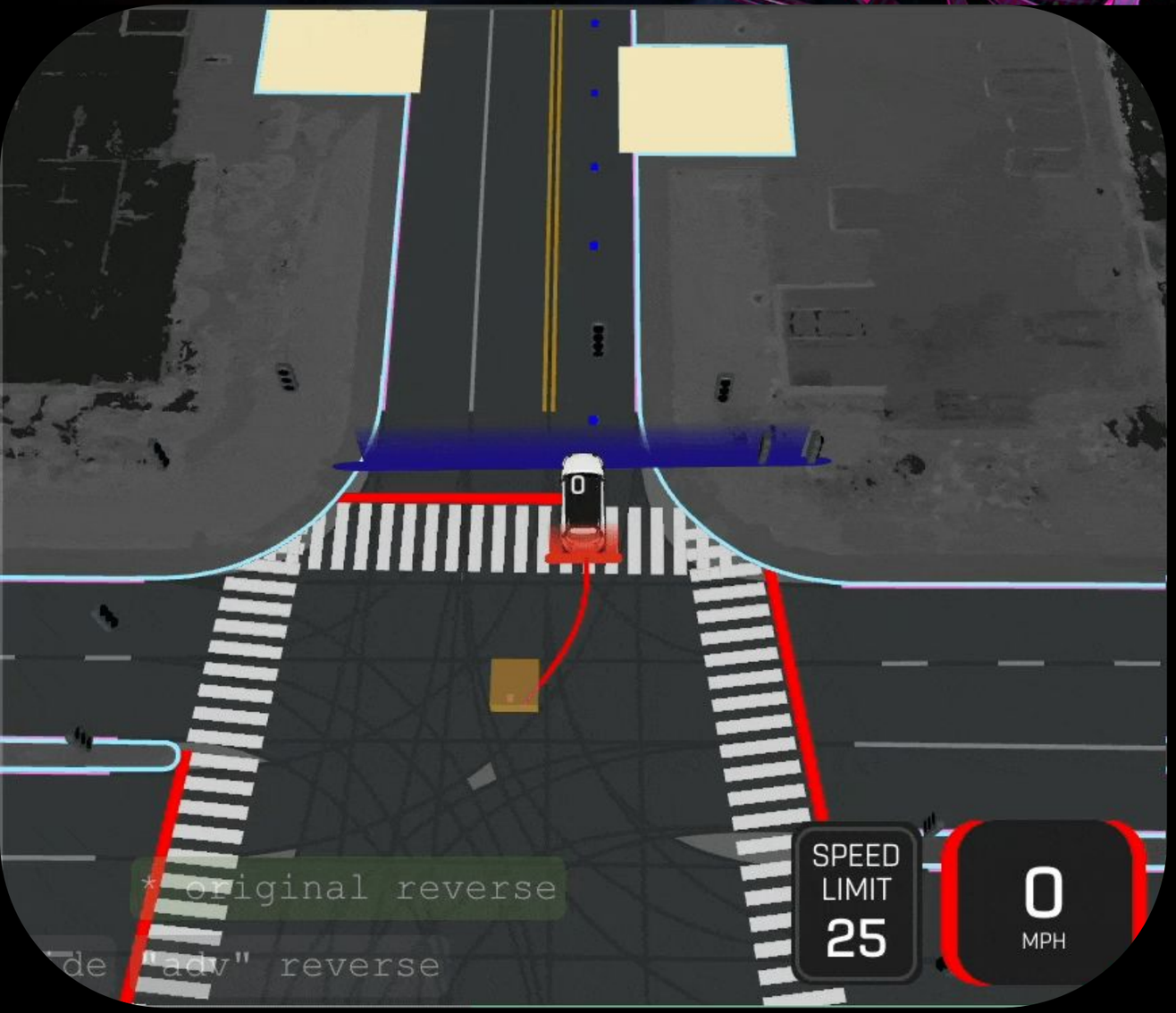


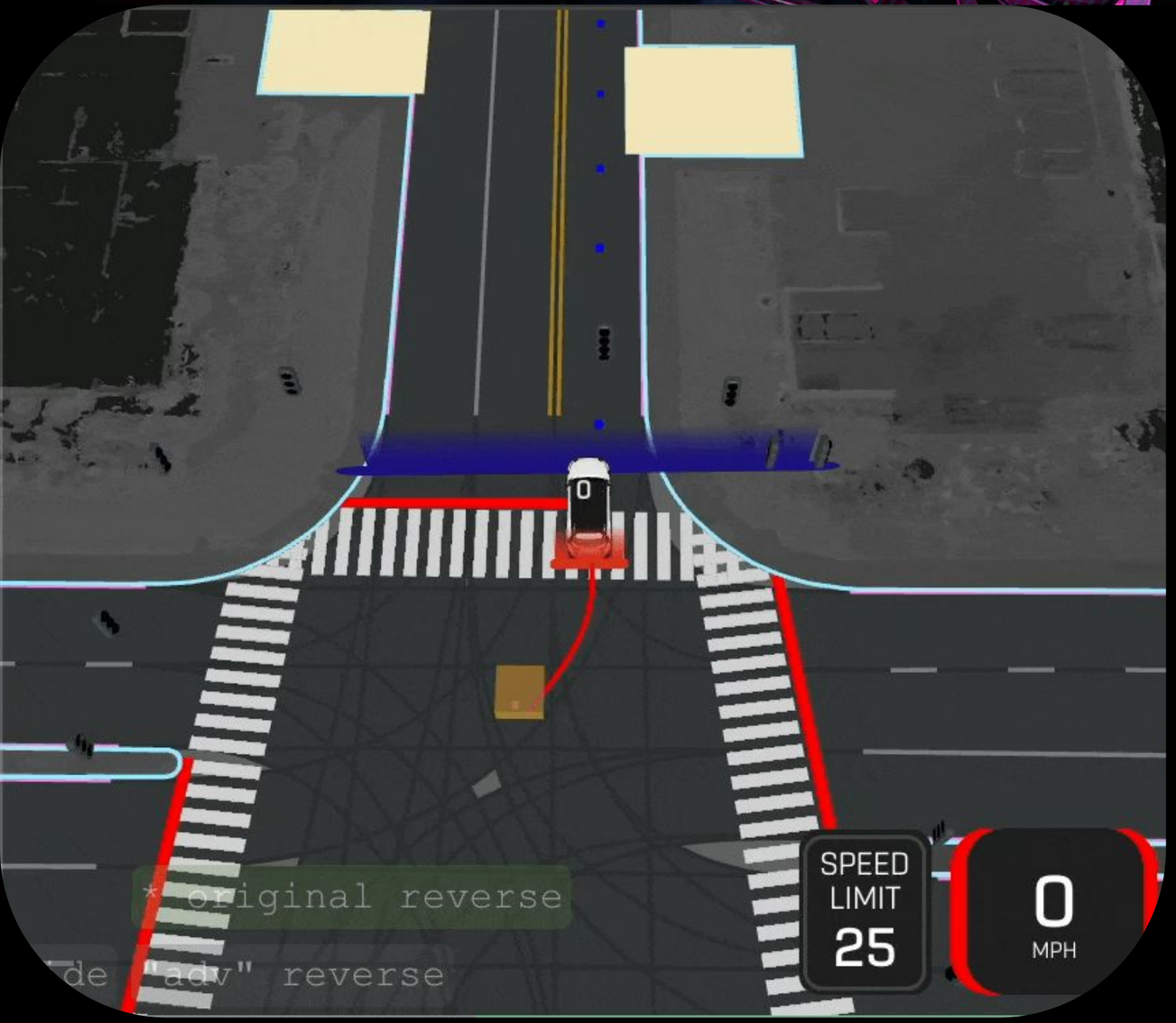
Situation type	Reversing in Intersection
AV maneuver	AV was driving forward away from the intersection
Agent maneuver	[Agent 1] behind AV, crossing intersection with the route
Command variants	Suggested reverse waypoint with new parameters • Start reversing timing (t)

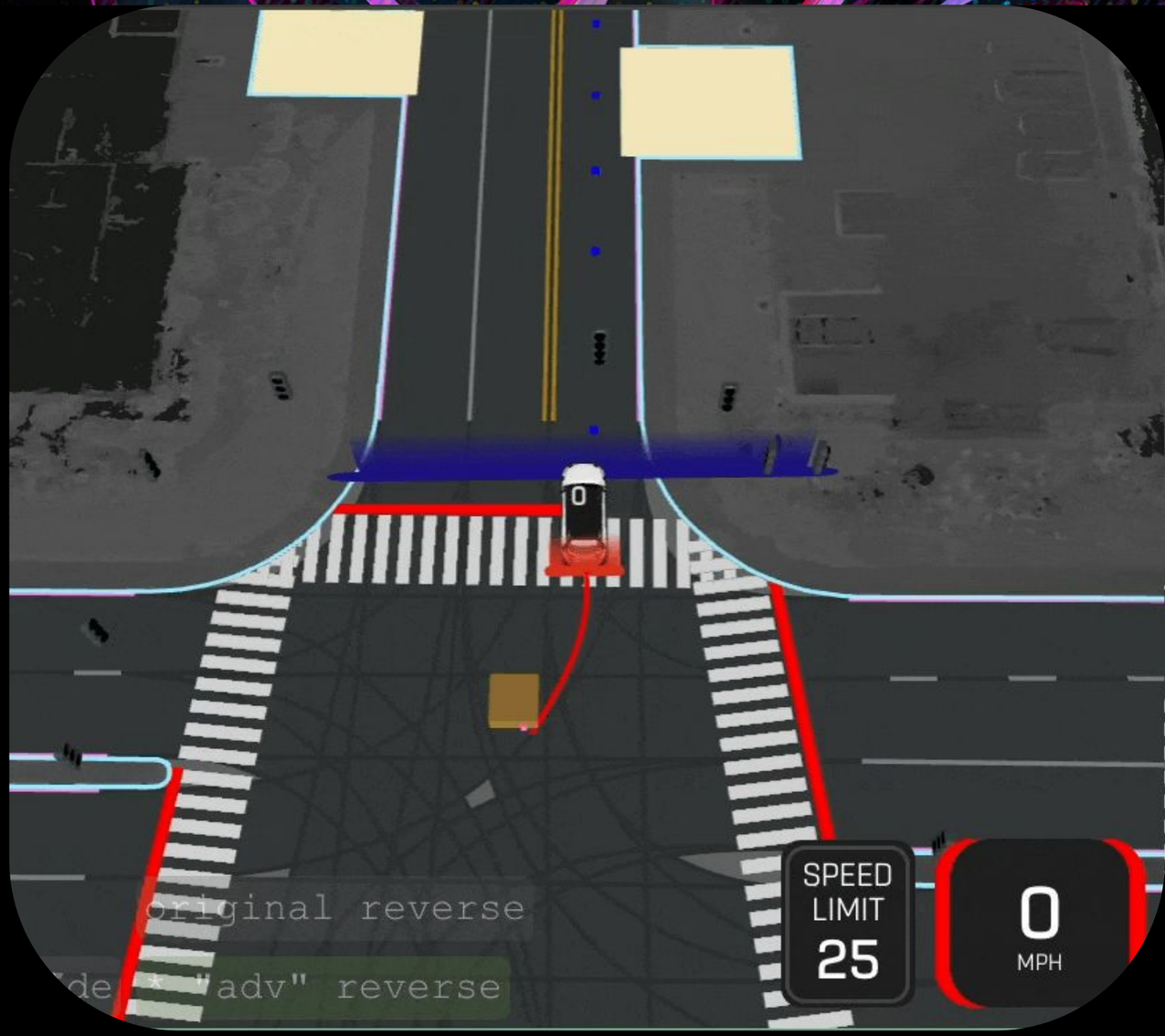
Case 2: Reversing in Intersection



Situation type	Reversing in Intersection
AV maneuver	AV was driving forward away from the intersection
Agent maneuver	[Agent 1] behind AV, crossing intersection with the route
Command variants	Suggested reverse waypoint with new parameters • Start reversing timing (t) • Destination longitudinal offset (x) • Destination lateral offset (y)


* original reverse
de "adv" reverse
SPEED LIMIT 25
0 MPH


SPEED LIMIT 25
0 MPH


SPEED LIMIT 25
0 MPH

Case 1

Merging from Parking

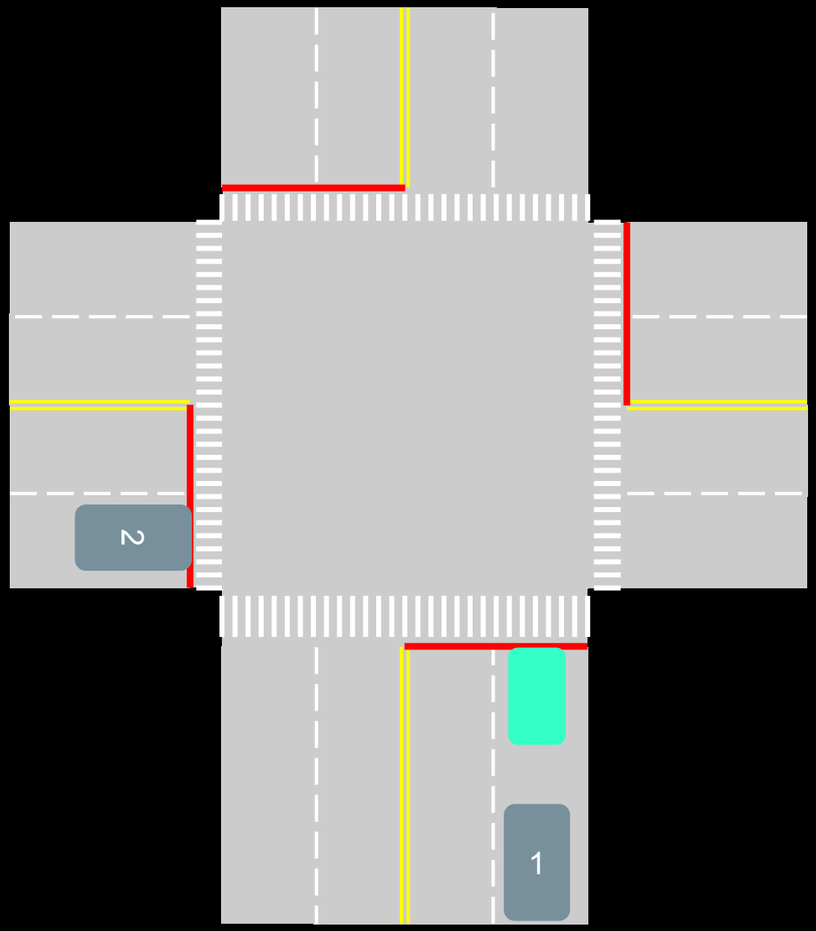
Case 2

Reversing into Intersection

Case 3

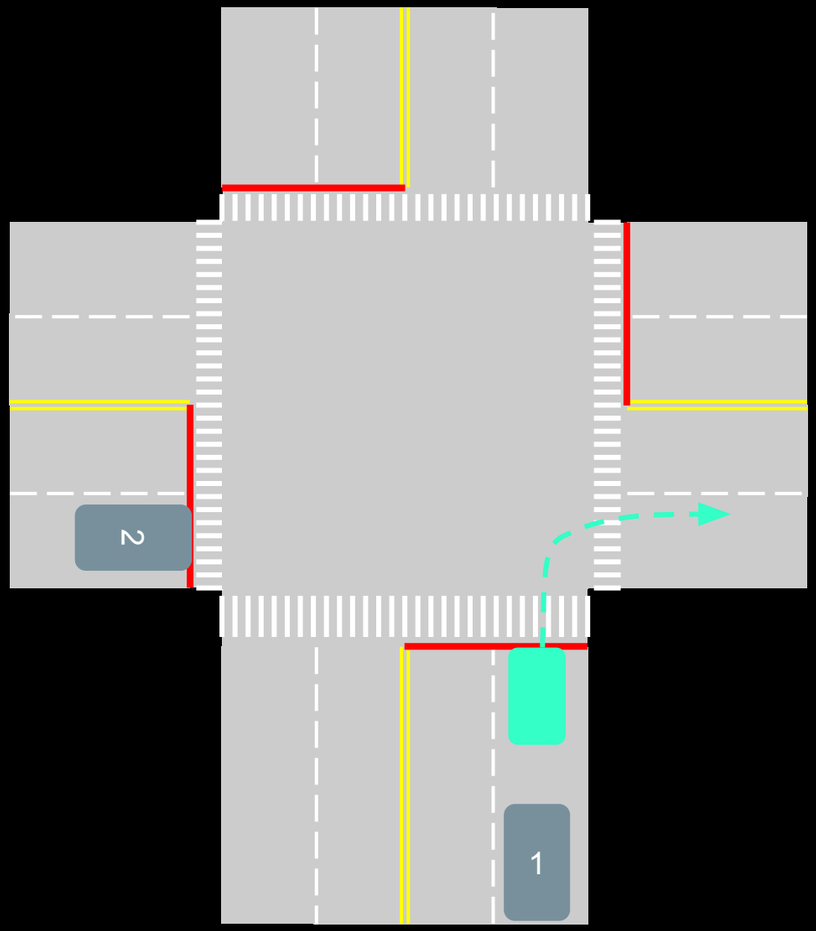
Right Turn with Multi-Agent Interaction

Case 3: Right Turn with Multi-Agent Interaction



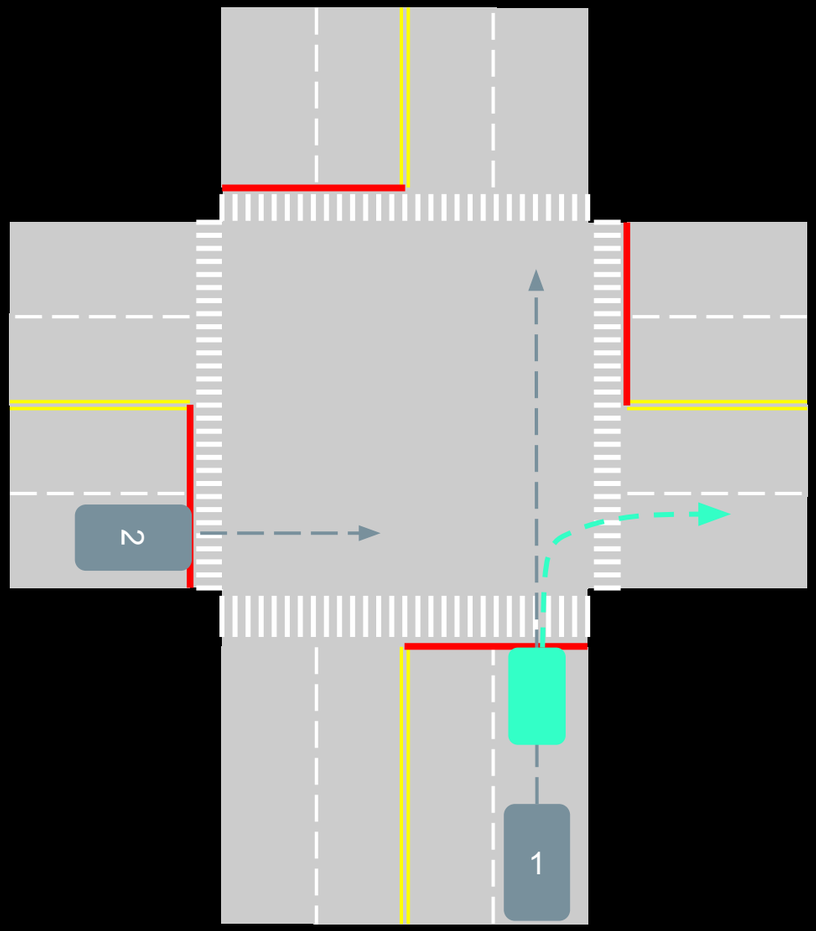
Situation type	Right Turn with Multi-Agent Interaction

Case 3: Right Turn with Multi-Agent Interaction



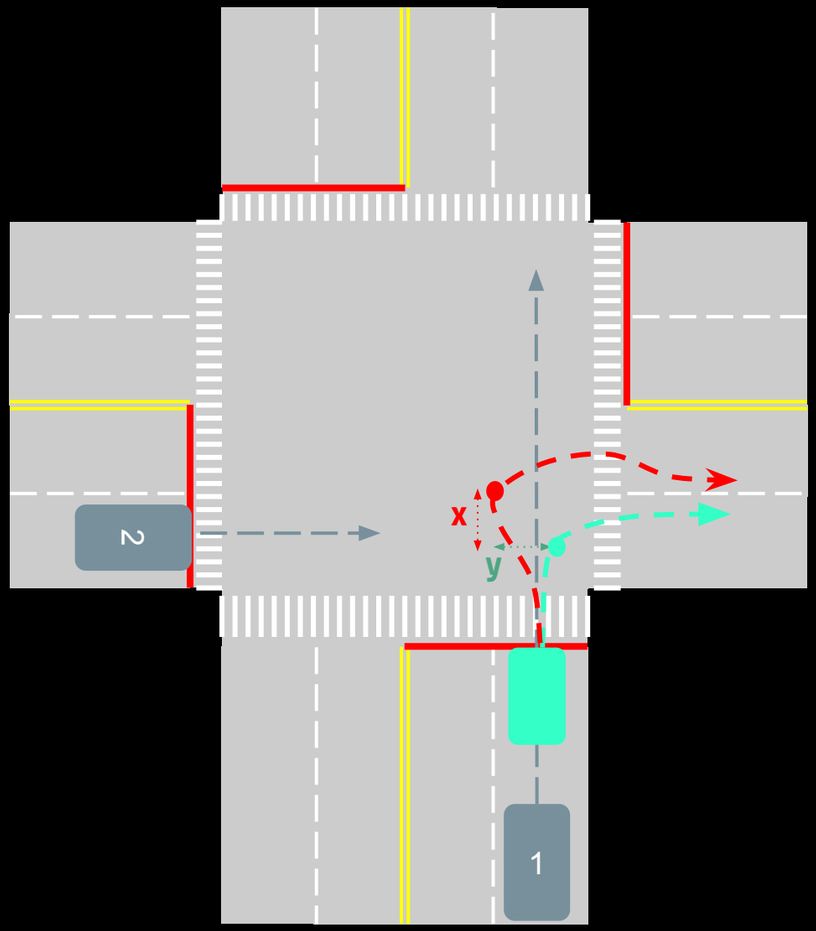
Situation type	Right Turn with Multi-Agent Interaction
AV maneuver	AV was following suggested waypoints to turn right through intersection

Case 3: Right Turn with Multi-Agent Interaction



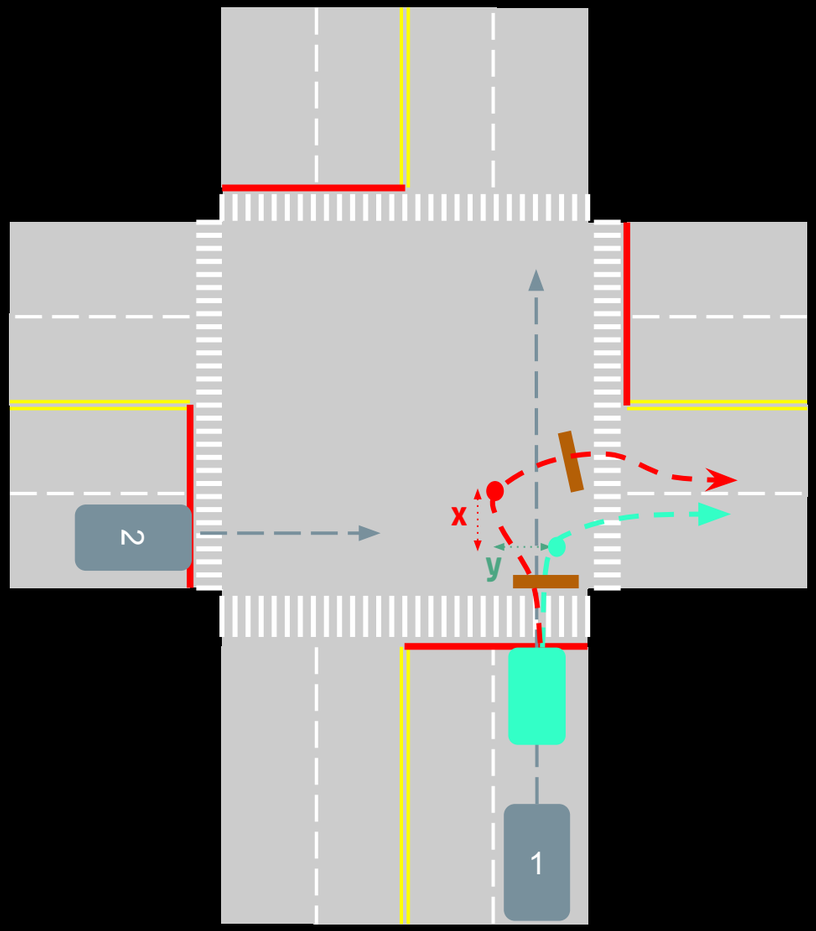
Situation type	Right Turn with Multi-Agent Interaction
AV maneuver	AV was following suggested waypoints to turn right through intersection
Agent maneuver	[Agent 1] behind AV, driving following the route [Agent 2] ahead of AV, driving following the route

Case 3: Right Turn with Multi-Agent Interaction



Situation type	Right Turn with Multi-Agent Interaction
AV maneuver	AV was following suggested waypoints to turn right through intersection
Agent maneuver	[Agent 1] behind AV, driving following the route [Agent 2] ahead of AV, driving following the route
Command variants	Suggested waypoints with new parameters • Longitudinal offset (x) • Lateral offset (y)

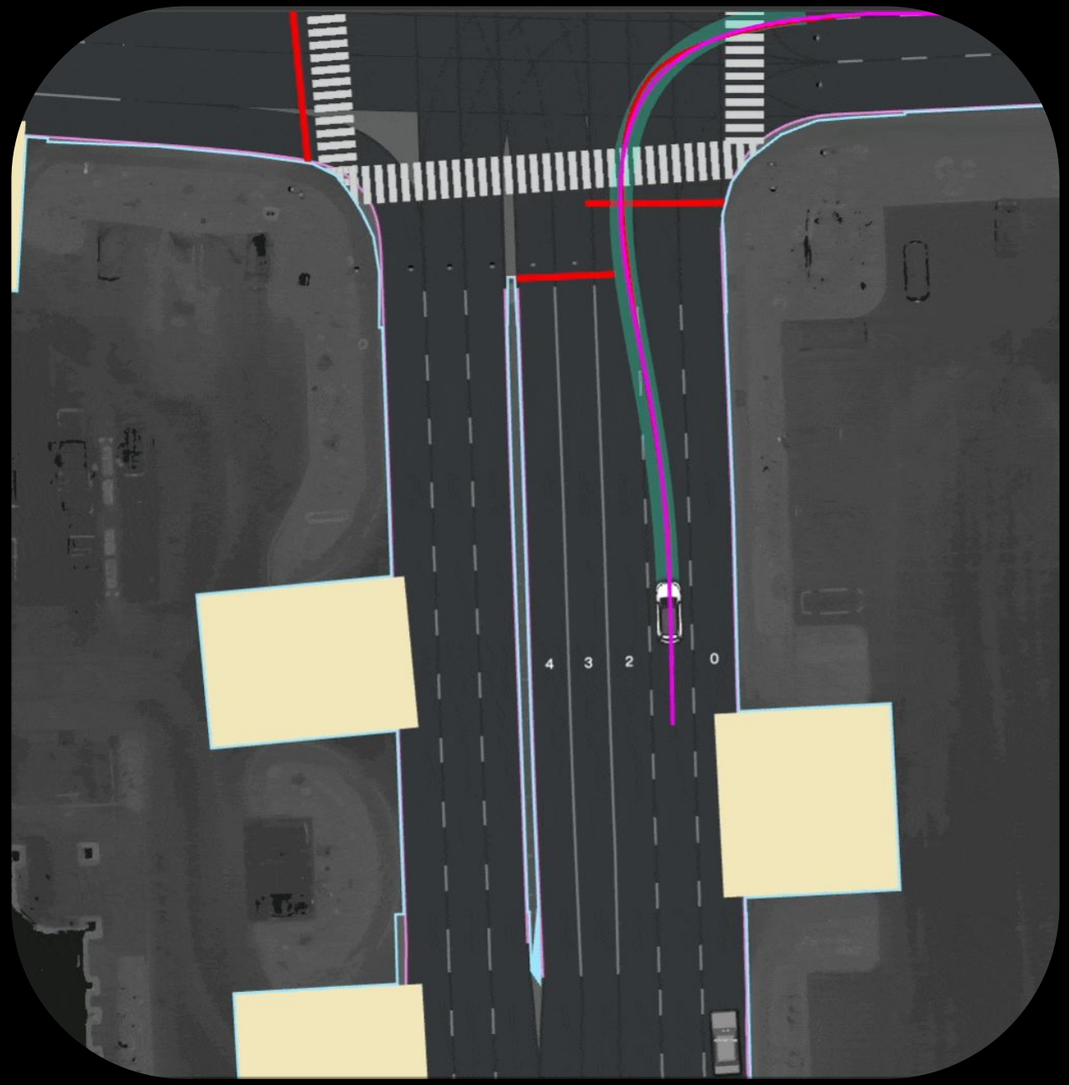
Case 3: Right Turn with Multi-Agent Interaction



Situation type	Right Turn with Multi-Agent Interaction
AV maneuver	AV was following suggested waypoints to turn right through intersection
Agent maneuver	[Agent 1] behind AV, driving following the route [Agent 2] ahead of AV, driving following the route
Command variants	Suggested waypoints with new parameters • Longitudinal offset (x) • Lateral offset (y) Emergency stop • Stop location (short bar)


4
3
2

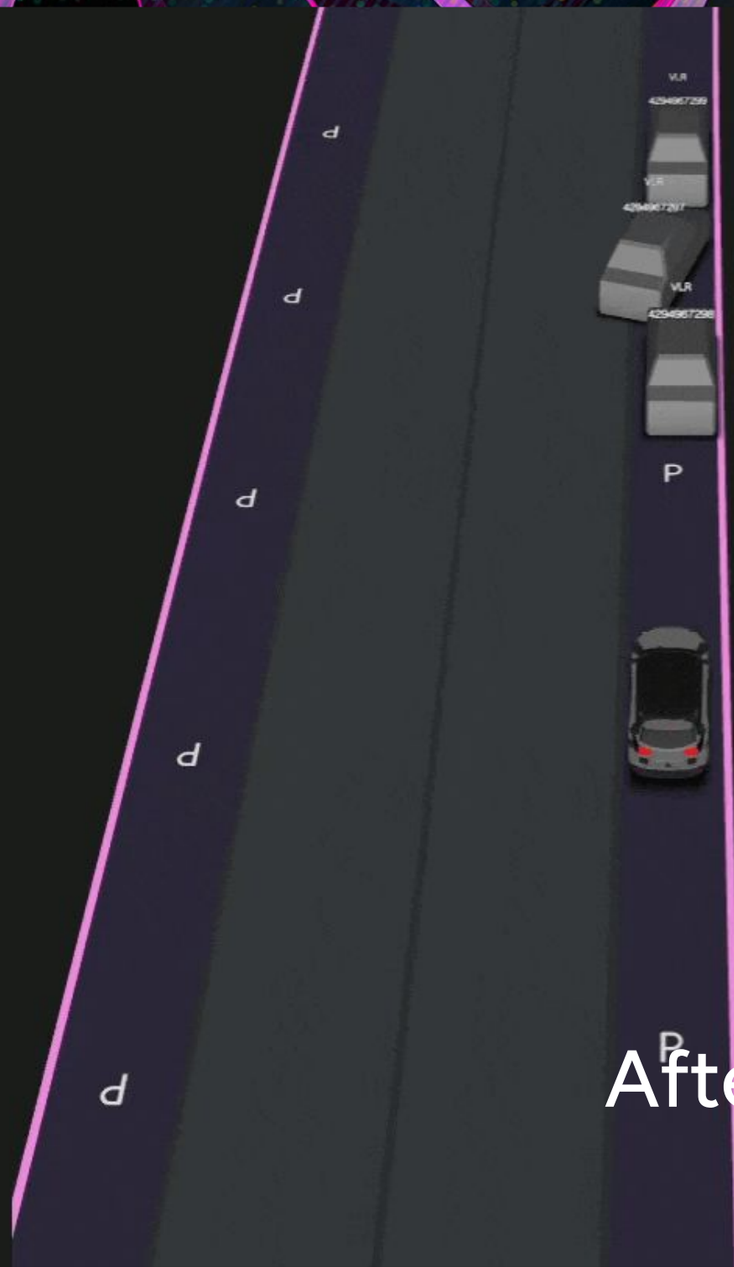

4 3 2


4 3 2 0

System improvement

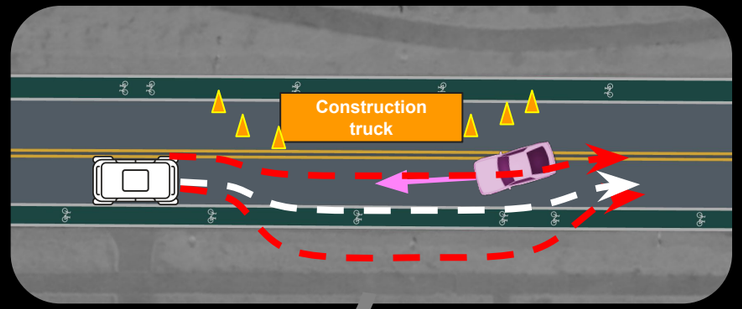
System improvement

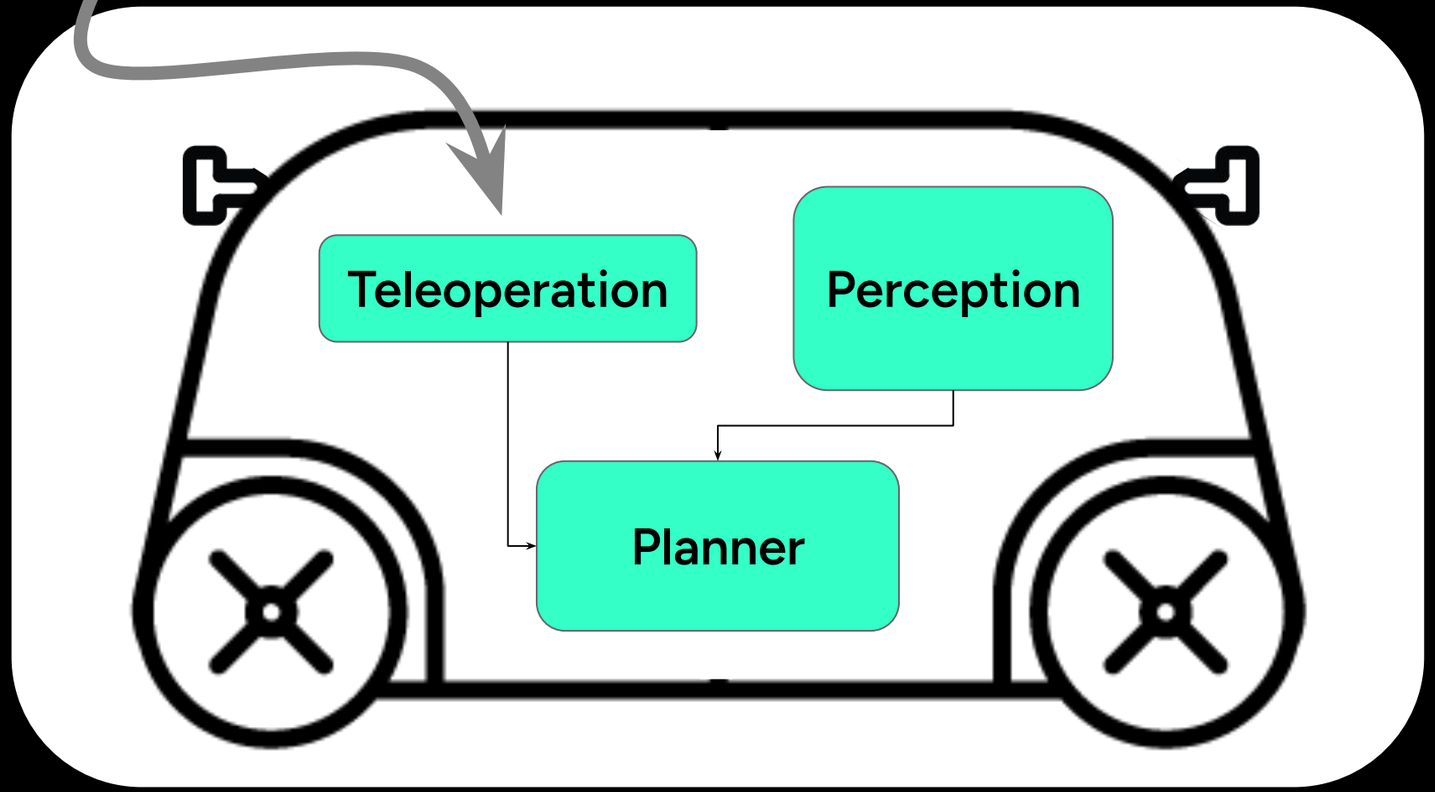
Before

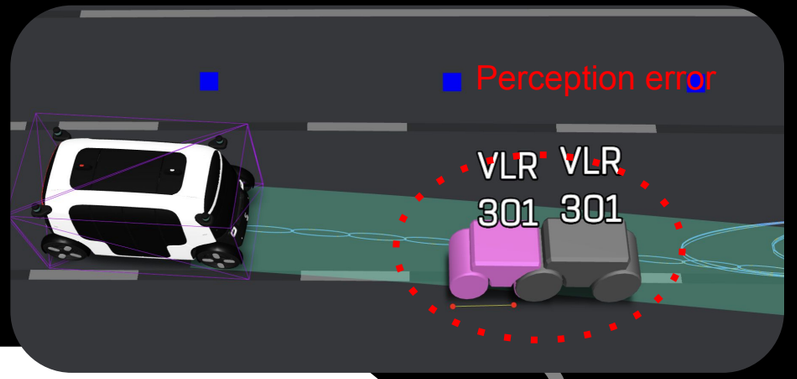


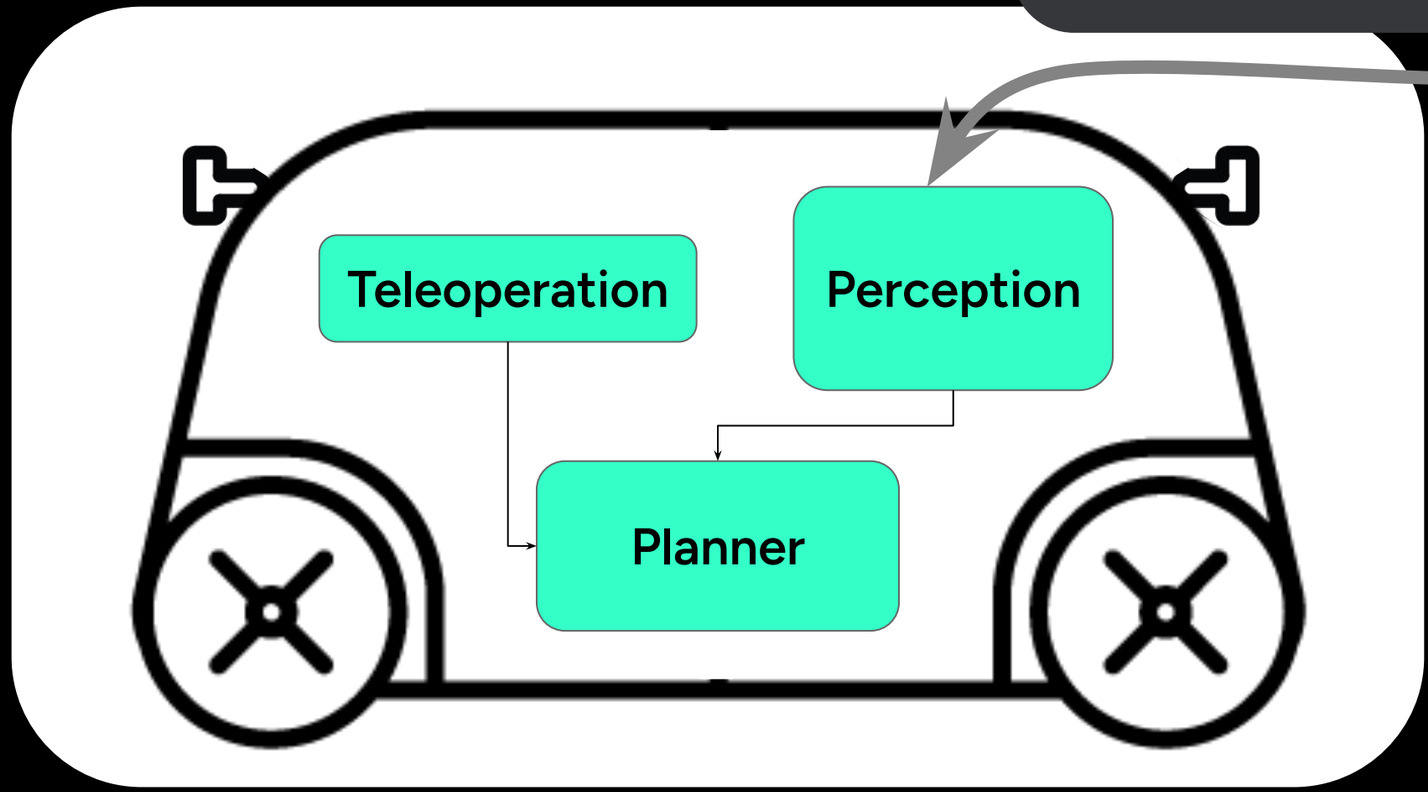
After

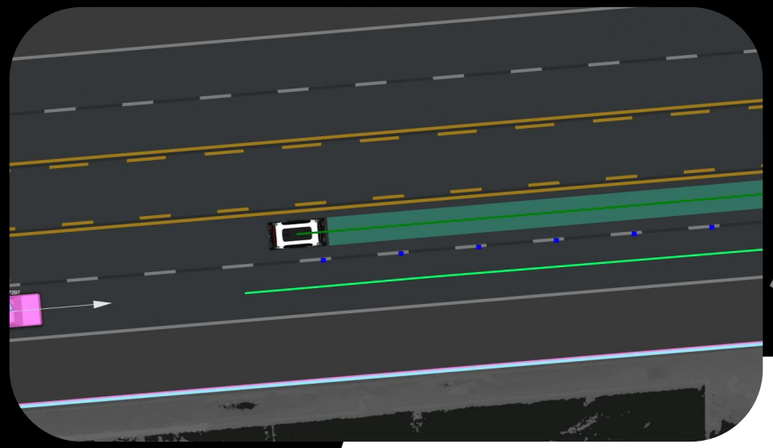
Looking Ahead

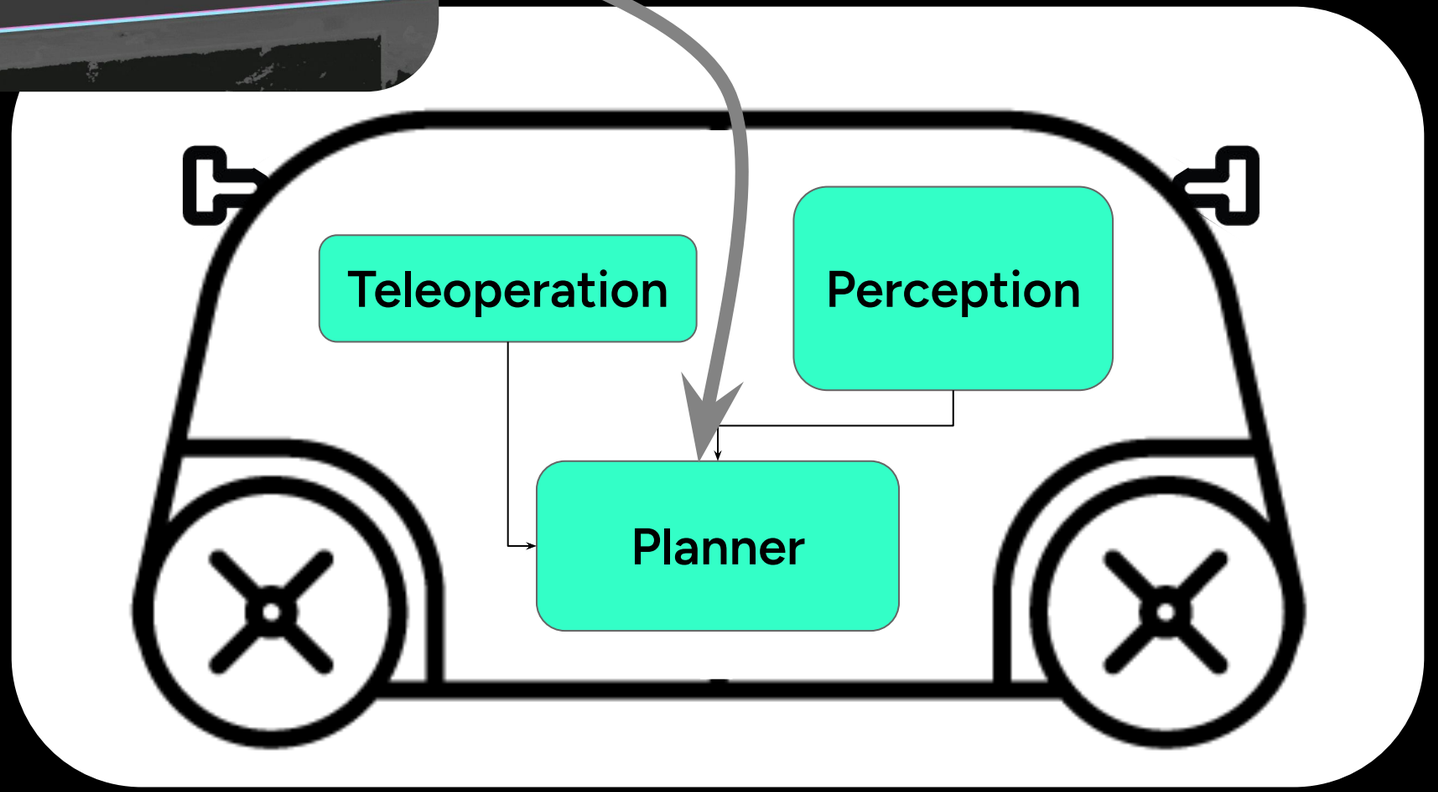

Construction truck


Teleoperation
Perception
Planner


Perception error
VLR 301
VLR 301


Teleoperation
Perception
Planner




Teleoperation
Perception
Planner

Safety Must Scale – Keep Fuzzing AI Stack

Zhisheng Hu ✉ zhu@zoox.com

Shanit Gupta
✉ shgupta@zoox.com

Thank You!