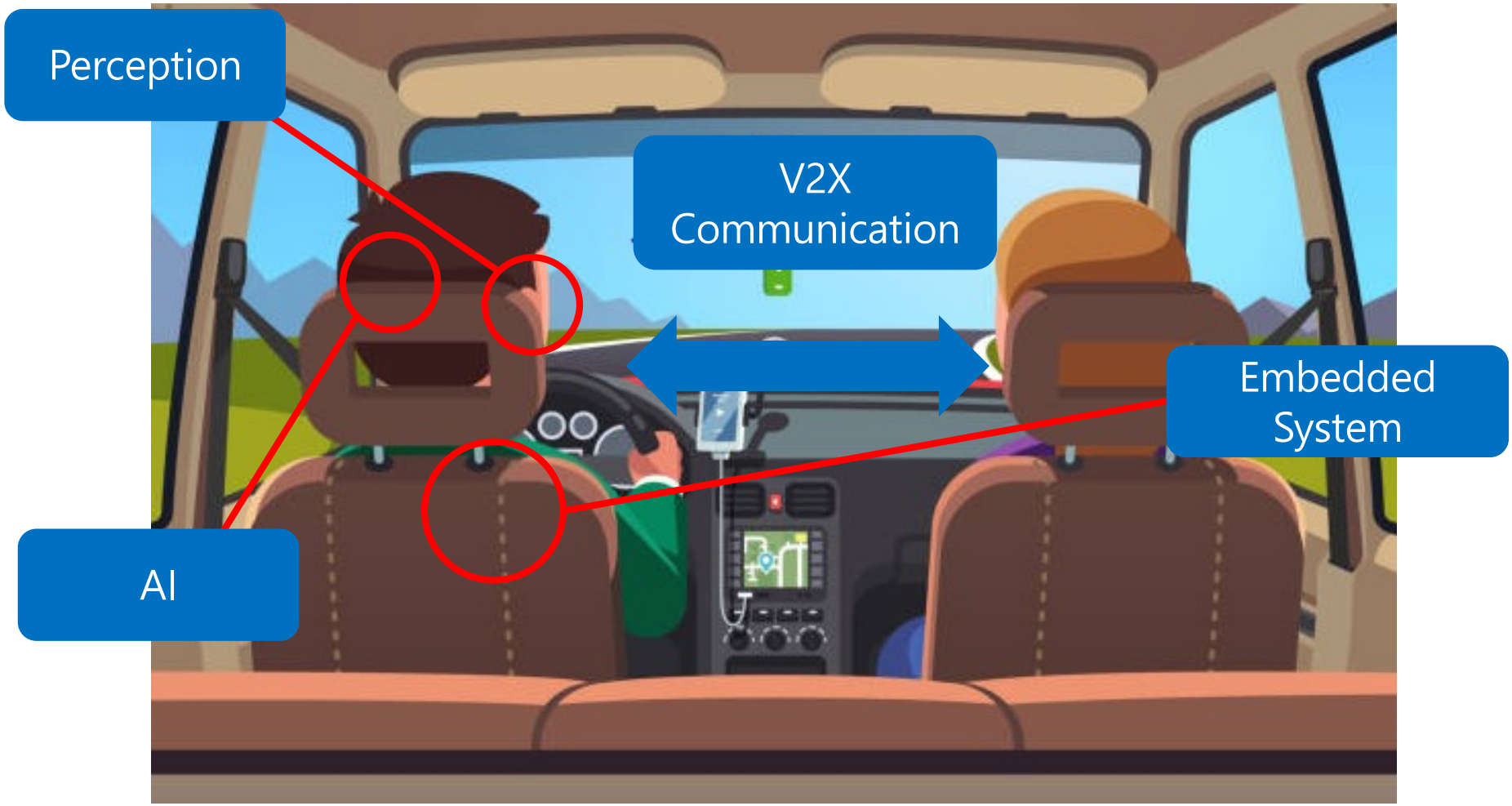
Attacking Self-driving Cars

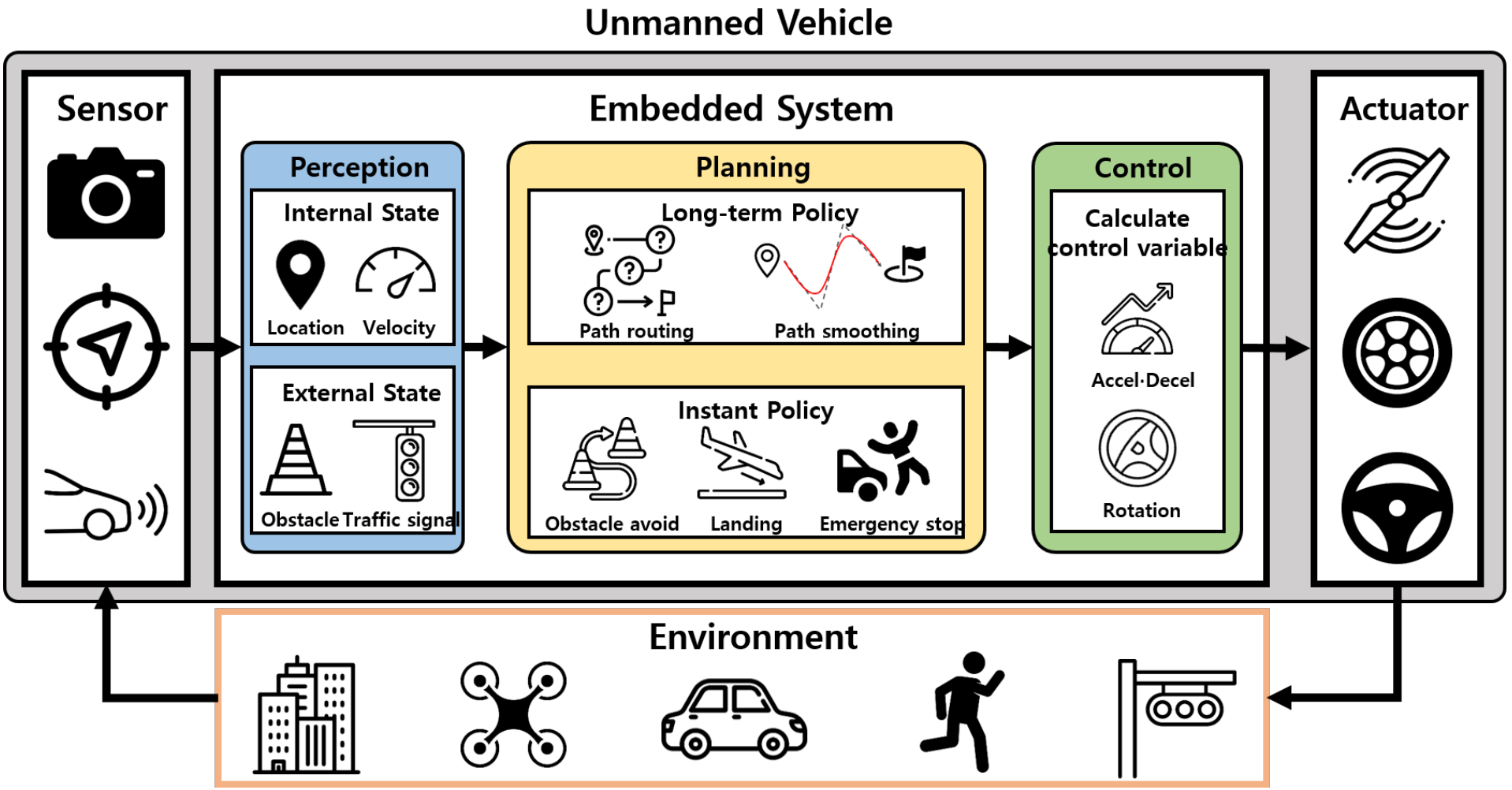
Yongdae Kim

SysSec@KAIST

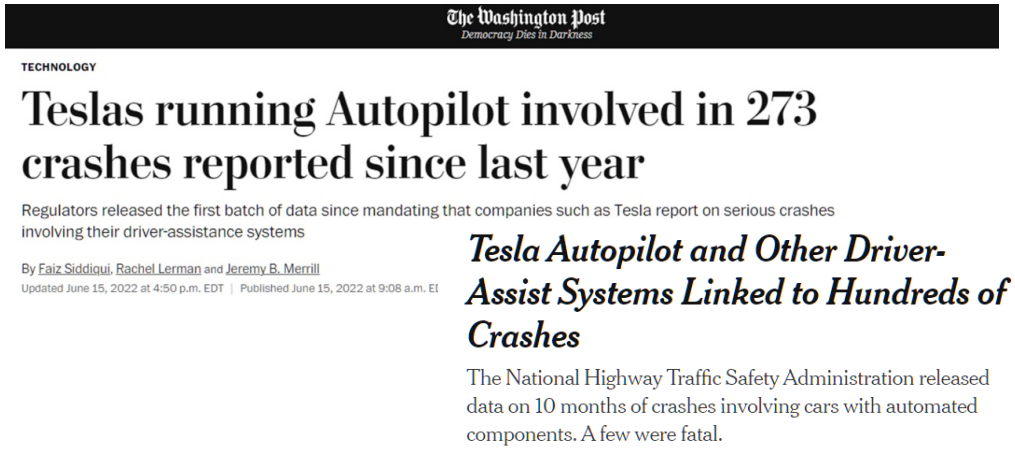
Manned vs Unmanned Vehicle



Unmanned Vehicle



Examples



The Washington Post
Democracy Dies in Darkness

TECHNOLOGY

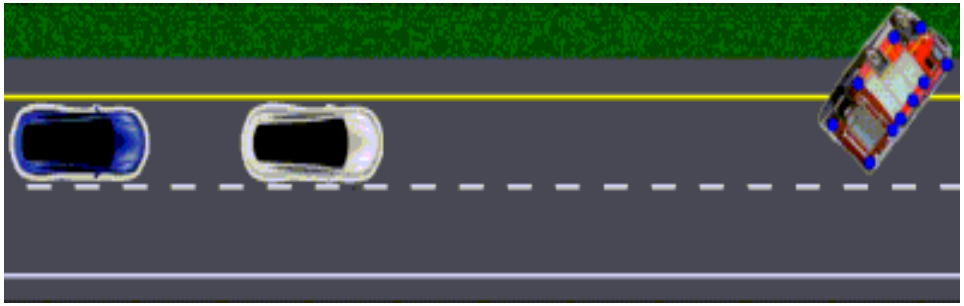
Teslas running Autopilot involved in 273 crashes reported since last year

Regulators released the first batch of data since mandating that companies such as Tesla report on serious crashes involving their driver-assistance systems

By Faiz Siddiqui, Rachel Lerman and Jeremy B. Merrill
Updated June 15, 2022 at 4:50 p.m. EDT | Published June 15, 2022 at 9:08 a.m. EI

Tesla Autopilot and Other Driver-Assist Systems Linked to Hundreds of Crashes

The National Highway Traffic Safety Administration released data on 10 months of crashes involving cars with automated components. A few were fatal.



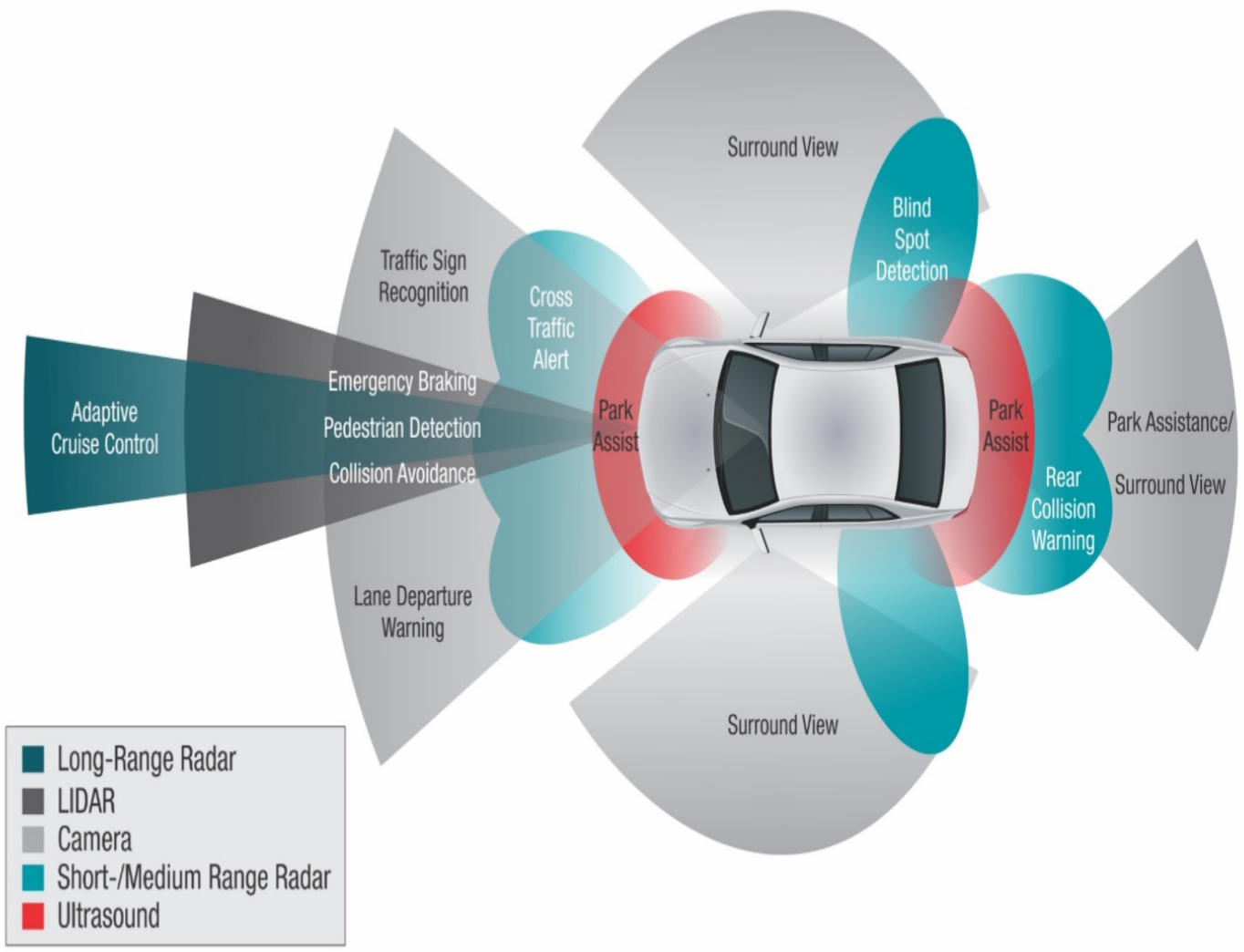
KAIST SysSec System Security Lab

A Few Fundamental Questions

- Definition of Safety with/without humans

- Safety under adversarial environment
  - What can/can't attacker control?
  - How can you define desired behaviors?
  - How can you define failures or undesired behaviors?
  - Fail-safe/Fault-tolerant?
  - Cost of achieving safety under adversarial environment?

Sensors for Autonomous Vehicles



❖ Proximity (5m).
: Ultrasonic sensors
(Parking assistance)

❖ Short Range (30m).
: Cameras, Short-range radars
(Traffic sign recognition, Parking assistance)

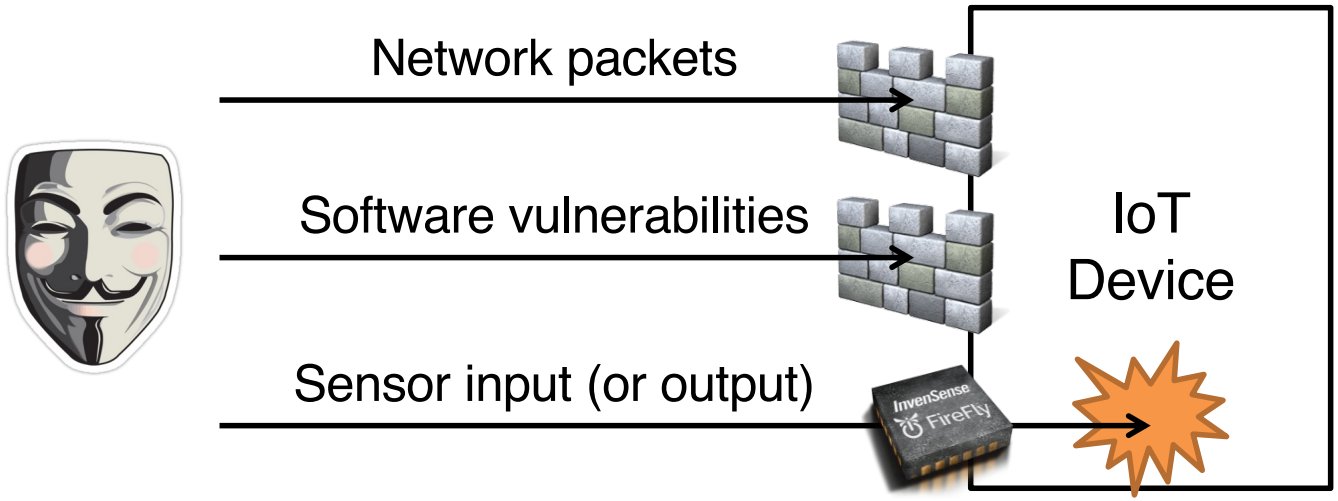
❖ Medium Range (80m)
: LiDAR and Medium range
radars (MRR)
(Collision avoidance, Pedestrian detection)

❖ Long Range (250m)
: Long-range radars (LRR)
(High speed)

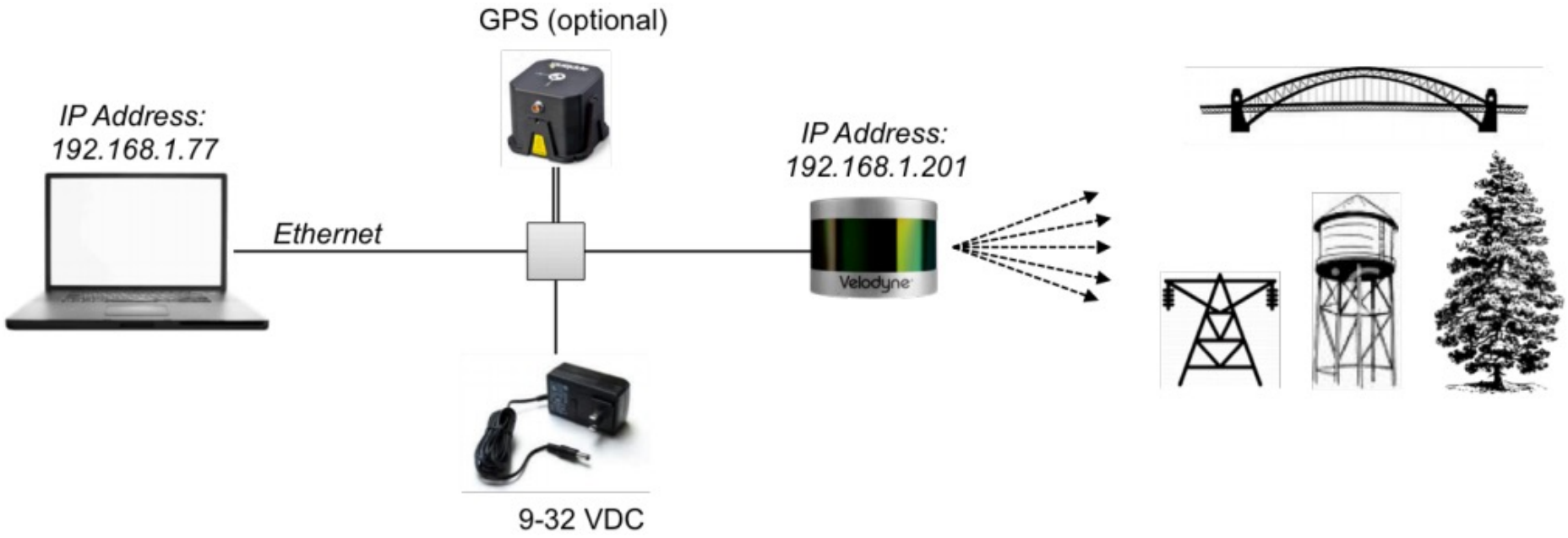
Sensor & Security

- Many prevention and detection mechanisms
  - For malicious network traffics
  - For software vulnerabilities

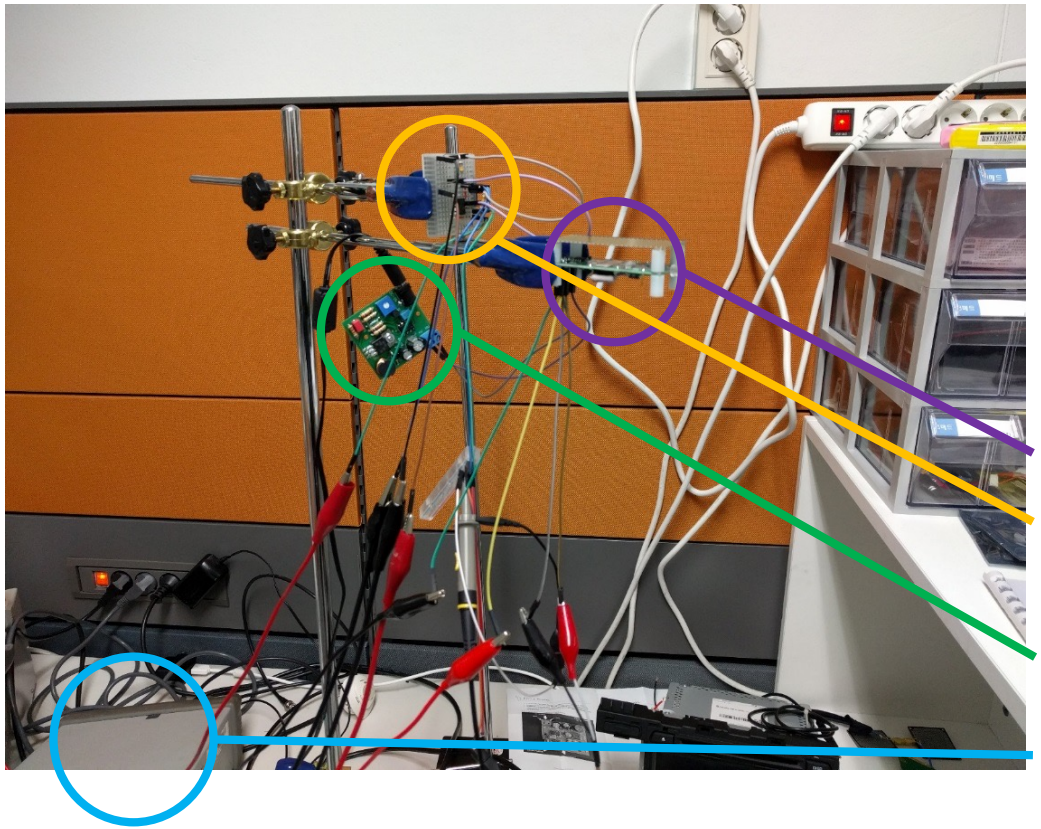
Sensor = A new attack vector

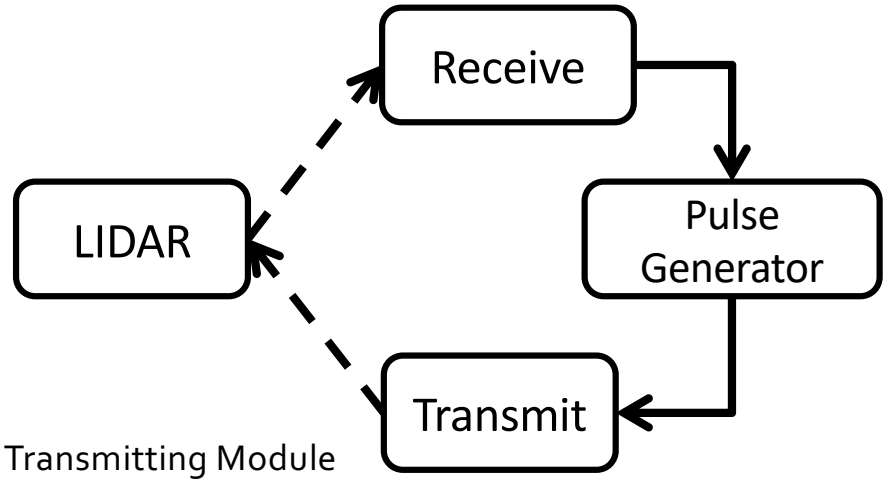


Velodyne VLP-16 [CHES'17]

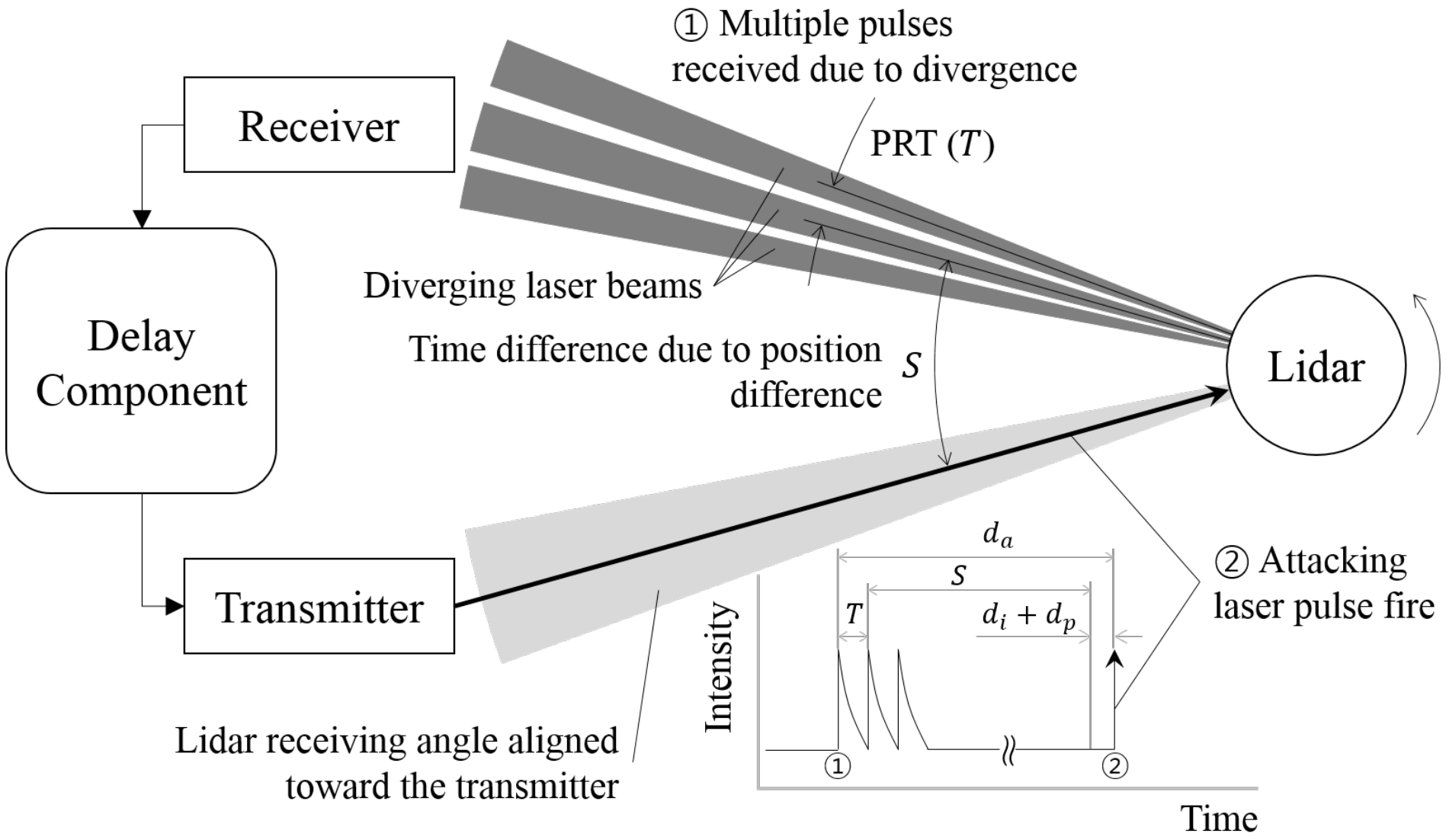


Velodyne VLP-16 Experimental Setting





Velodyne VLP-16: Fundamental Idea

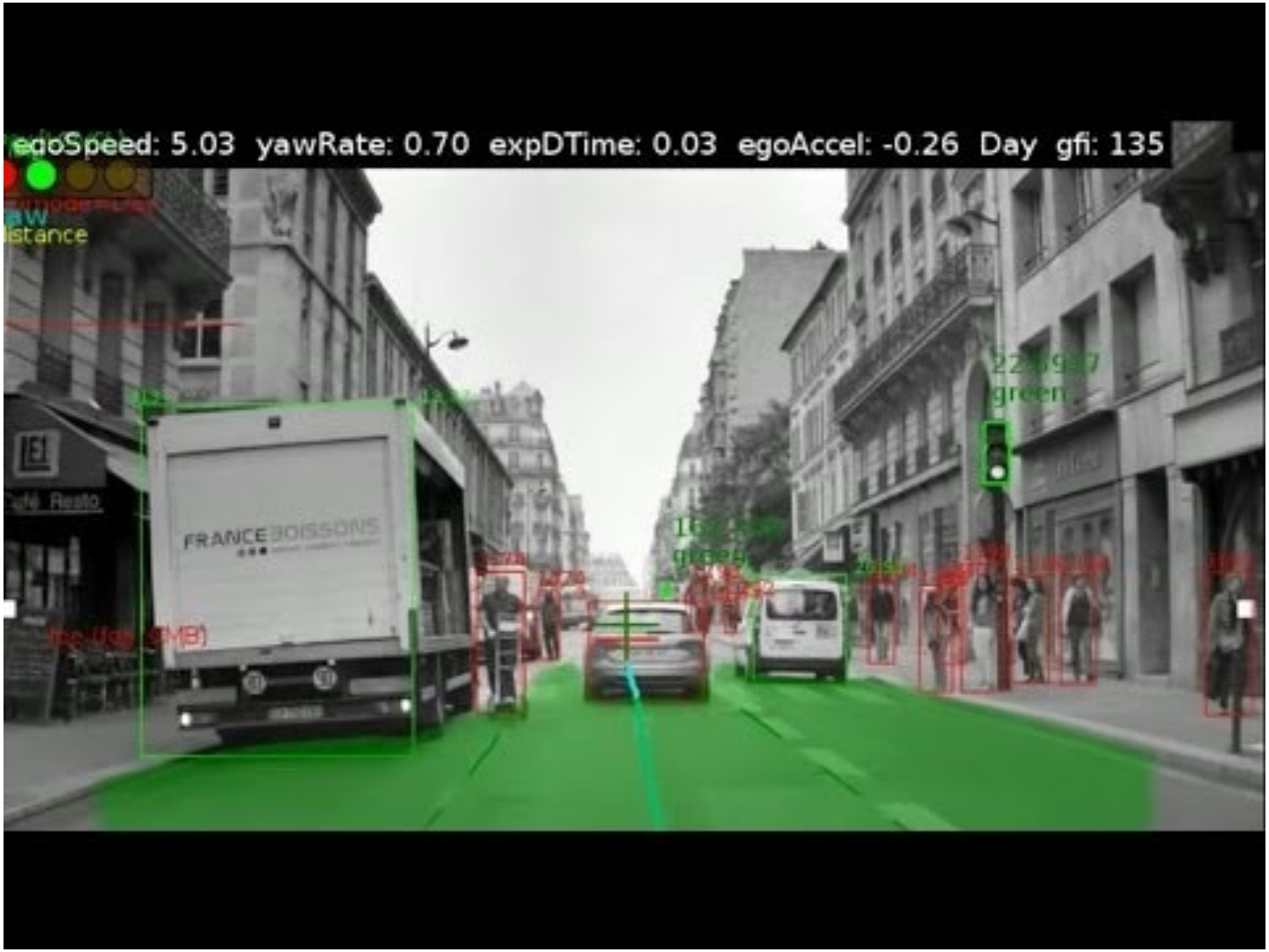


VLP-16 Experiment

Curved Surface

VLP-16 Experiment

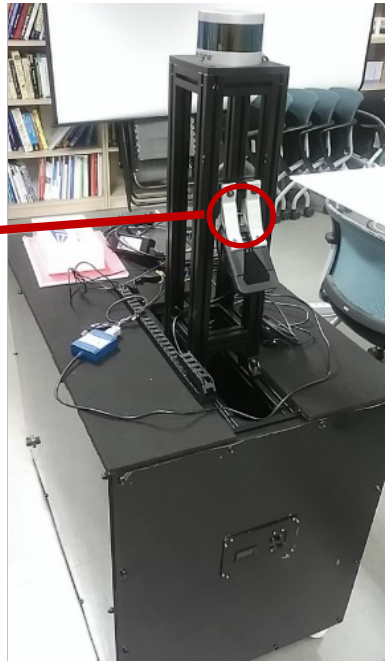
Mobileye



- GM
- BMW
- Nissan
- Volvo
- (over 19 in total)

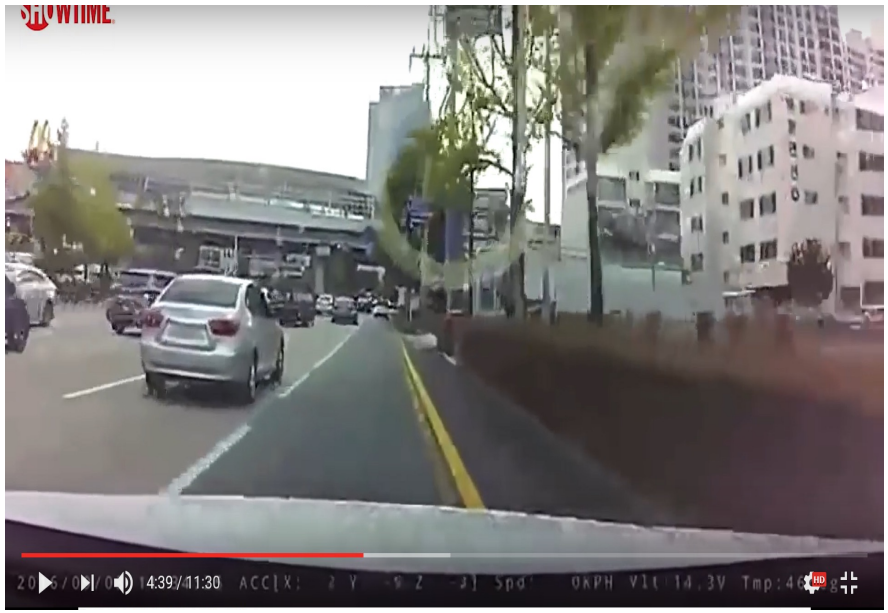
Mobileye-560 [Unpublished]

- Classify the objects
  - Vehicle, Pedestrian, Truck, Bike, Bicycle, Sign, Lane etc.
- Information about the Object
  - Distance, Velocity, State, etc.
- Recognition range : ~80m
- Black and White screen



Parser

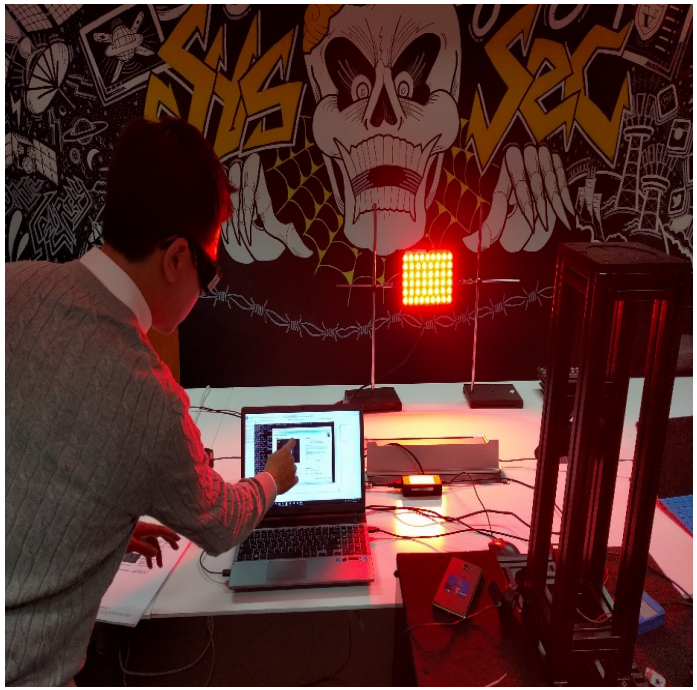
Parser prints the results for black box video.
(Object classification, velocity, accelerometer …)



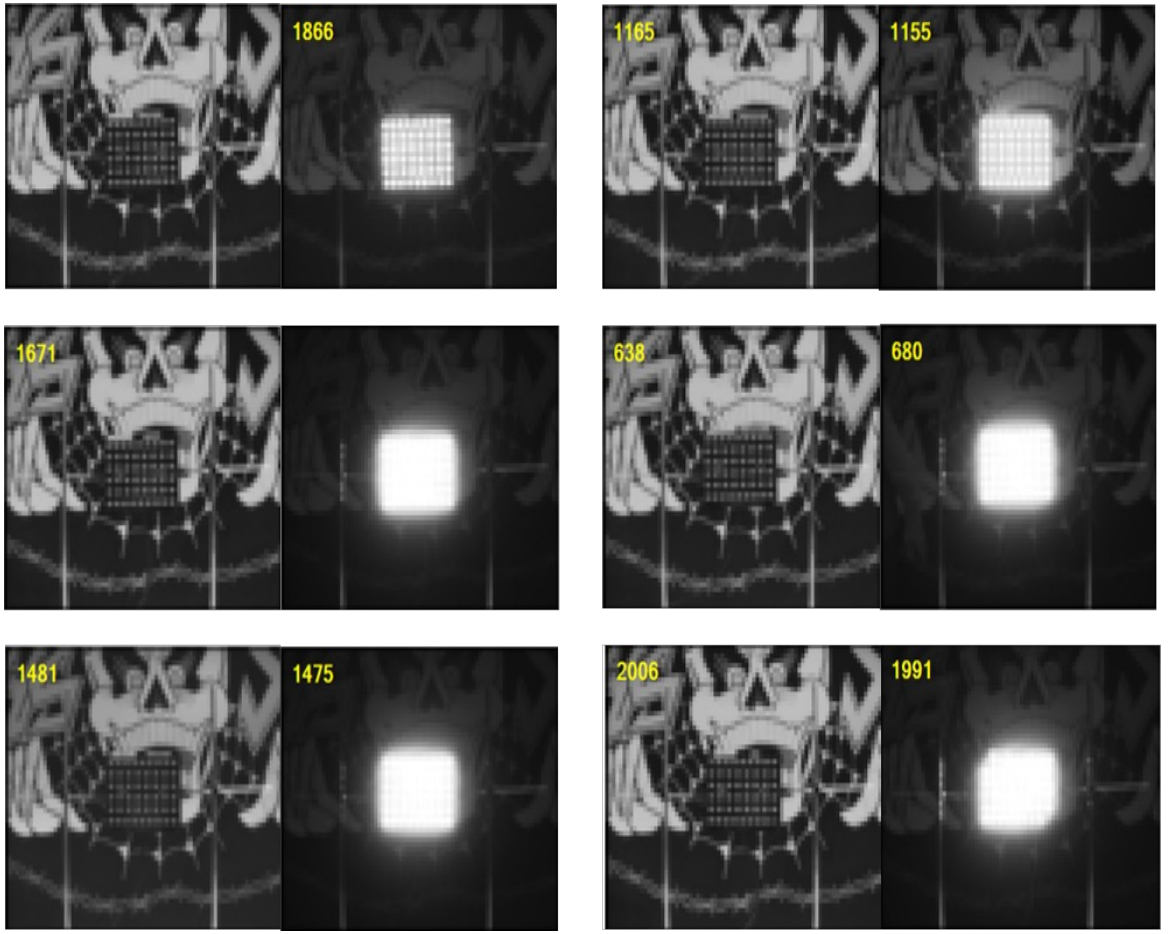
C:₩Users₩SysSec-EE₩Desktop₩CAN Receive₩.₩Debug₩CAN Receive.exe

```
Num_Obstacles : 2
STOP!!!
Existing object

Obstacle is Vehicle
Obstacle parked
Obstacle      X: 16.625 m,      Y: -1.938 m
Obstacle  vel_X: -0.000
Obstacle length: 31.500 m, width: 1.450 m

Obstacle age: 254
Obstacle lane not assigned
Obstacle angle rate: -0.210 deg/sec, scale change: 0.001 pix/sec

Obstacle acc: -0.480 m/s2

Obstacle angle: -321.020 deg

Existing object

Obstacle is Bike
Obstacle is standing
Obstacle      X: 47.313 m,      Y: 2.930 m
Obstacle  vel_X: -0.000
Obstacle length: 31.500 m, width: 0.600 m

Obstacle age: 254
Obstacle lane not assigned
Obstacle angle rate: 0.110 deg/sec, scale change: -0.003 pix/sec
```

Blinding Attack (Visible Light)

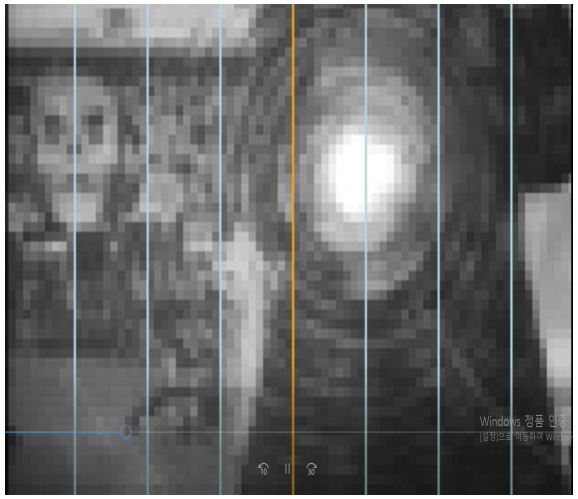


Experiment setup



980nm, 385nm, 460nm, 520nm, 585nm, 620nm

Invisible Light (IR)

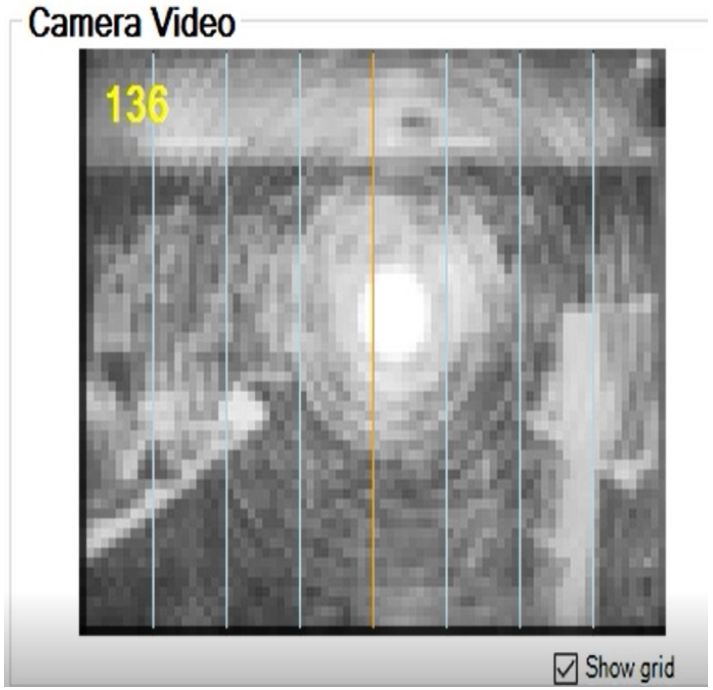


780nm 3mW Laser module: **Blinding!**

780nm 100mW Laser module

Camera

Blinding!

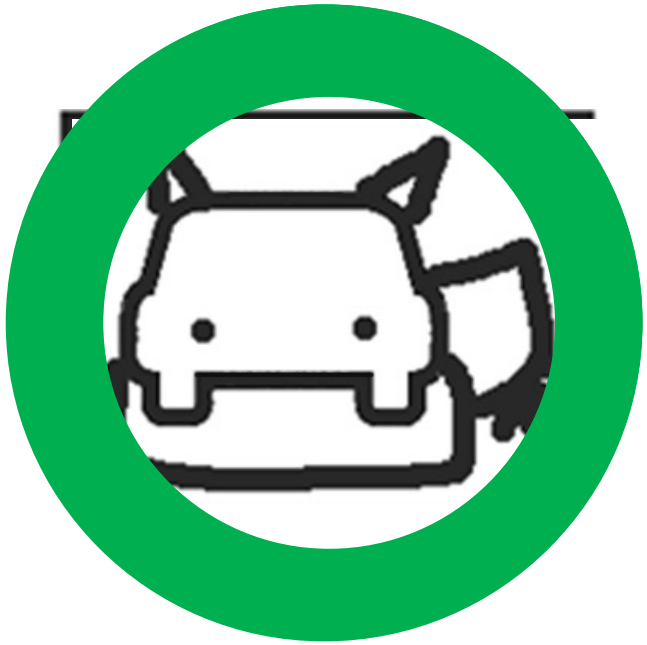


3. Camera module blinded by laser injection

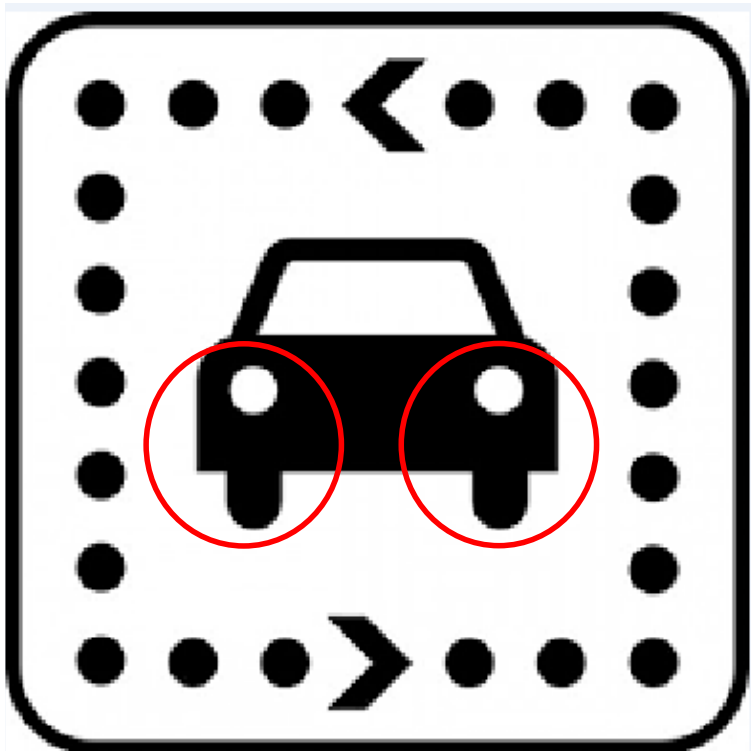
Mobileye Classification

Are You Serious?

Variations



Men in the Car



GPS Spoofing

KAIST SysSec System Security Lab

Blinding AEB

Tesla Model S

Camera Blinding Effect on AEB

Demo

GPS Spoofing and Auto-pilot

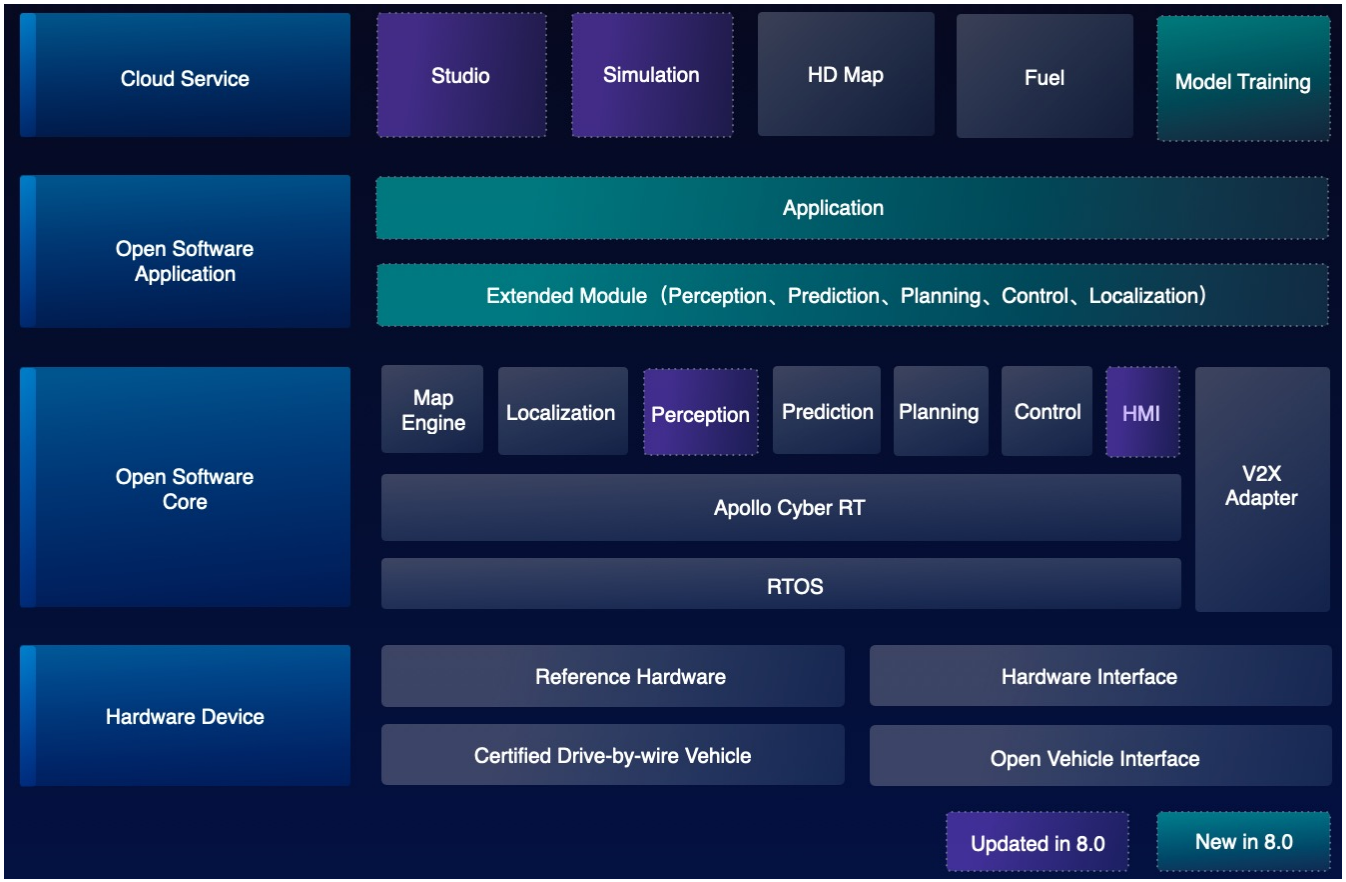
GPS Spoofing Effect on
Tesla Autopilot Cruise Speed

DoS Using Fake Base Station

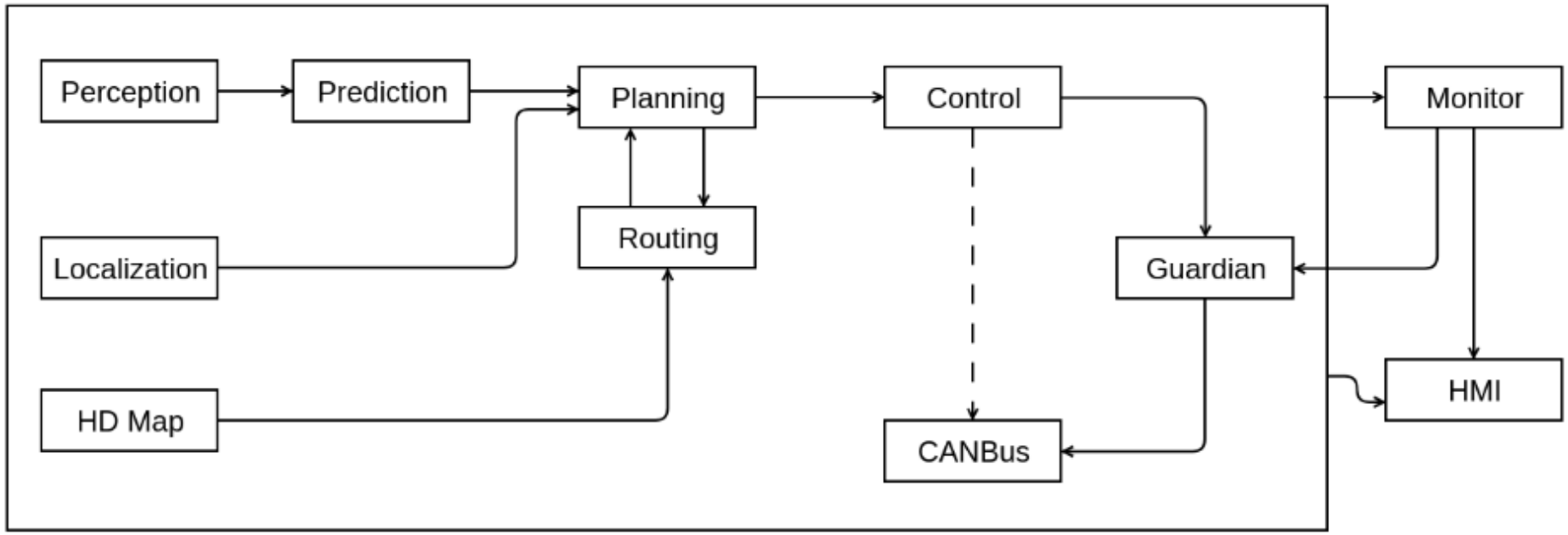
Denial of Service attack using
FAKE base station

Planning - Control

Baidu Apollo Overview

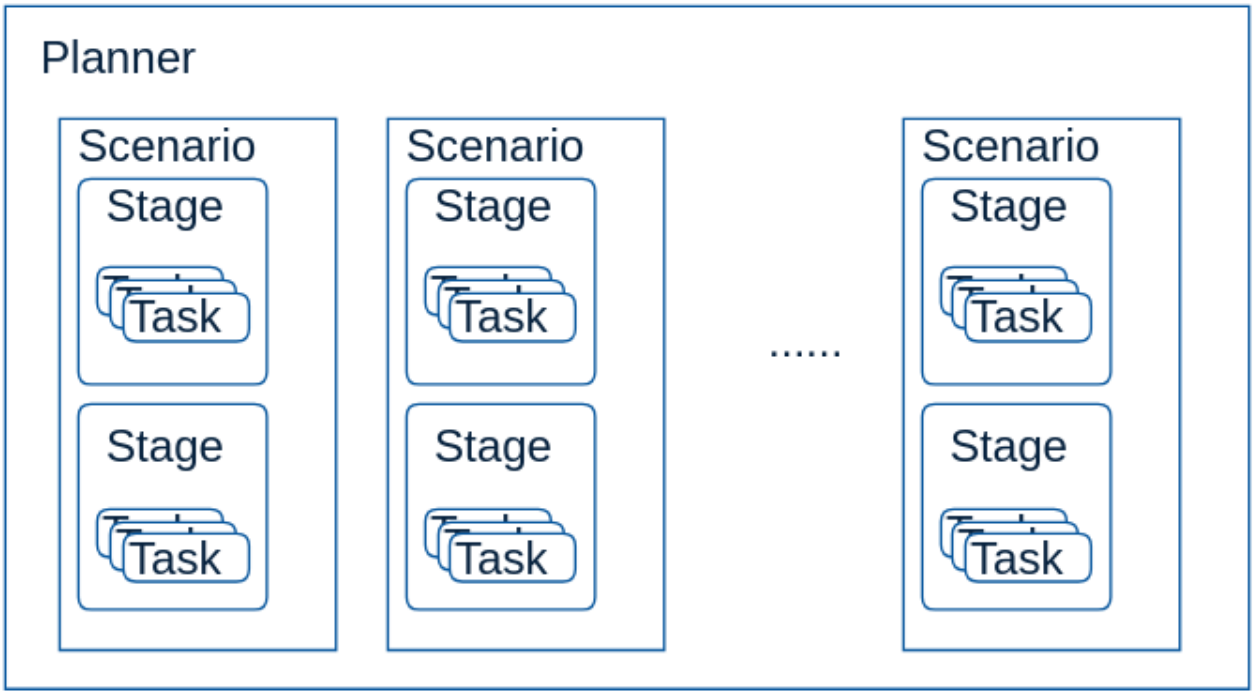


Apollo Software Overview



Apollo Software Overview

- Stage, and Task are executed sequentially
  - Scene does not change until current scene is finished
- In single frame, current scene and stage is determined
  - Pre-defined list of task are executed




```
scenario_type: TRAFFIC_LIGHT_PROTECTED
traffic_light_protected_config: {
  start_traffic_light_scenario_distance: 5.0
  max_valid_stop_distance: 2.0
  min_pass_s_distance: 3.0
}
stage_type: TRAFFIC_LIGHT_PROTECTED_APPROACH
stage_type: TRAFFIC_LIGHT_PROTECTED_INTERSECTION_CRUISE

stage_config: {
  stage_type: TRAFFIC_LIGHT_PROTECTED_APPROACH
  enabled: true
  task_type: PATH_LANE_BORROW_DECIDER
  task_type: PATH_BOUNDS_DECIDER
  task_type: PIECEWISE_JERK_PATH_OPTIMIZER
  task_type: PATH_ASSESSMENT_DECIDER
  task_type: PATH_DECIDER
  task_type: RULE_BASED_STOP_DECIDER
  task_type: ST_BOUNDS_DECIDER
  task_type: SPEED_BOUNDS_PRIORI_DECIDER
  task_type: SPEED_HEURISTIC_OPTIMIZER
  task_type: SPEED_DECIDER
  task_type: SPEED_BOUNDS_FINAL_DECIDER
  task_type: PIECEWISE_JERK_NONLINEAR_SPEED_OPTIMIZER
  task_config: {
    task_type: PATH_LANE_BORROW_DECIDER
  }
```

Security Standard for Vehicles

- ISO 26262
  - Road vehicles — Functional safety:
  - Focus on E/E system failure

- Decision-making algorithms begin to be installed in ADS
  - The need for verification of functional insufficiencies begins to emerge

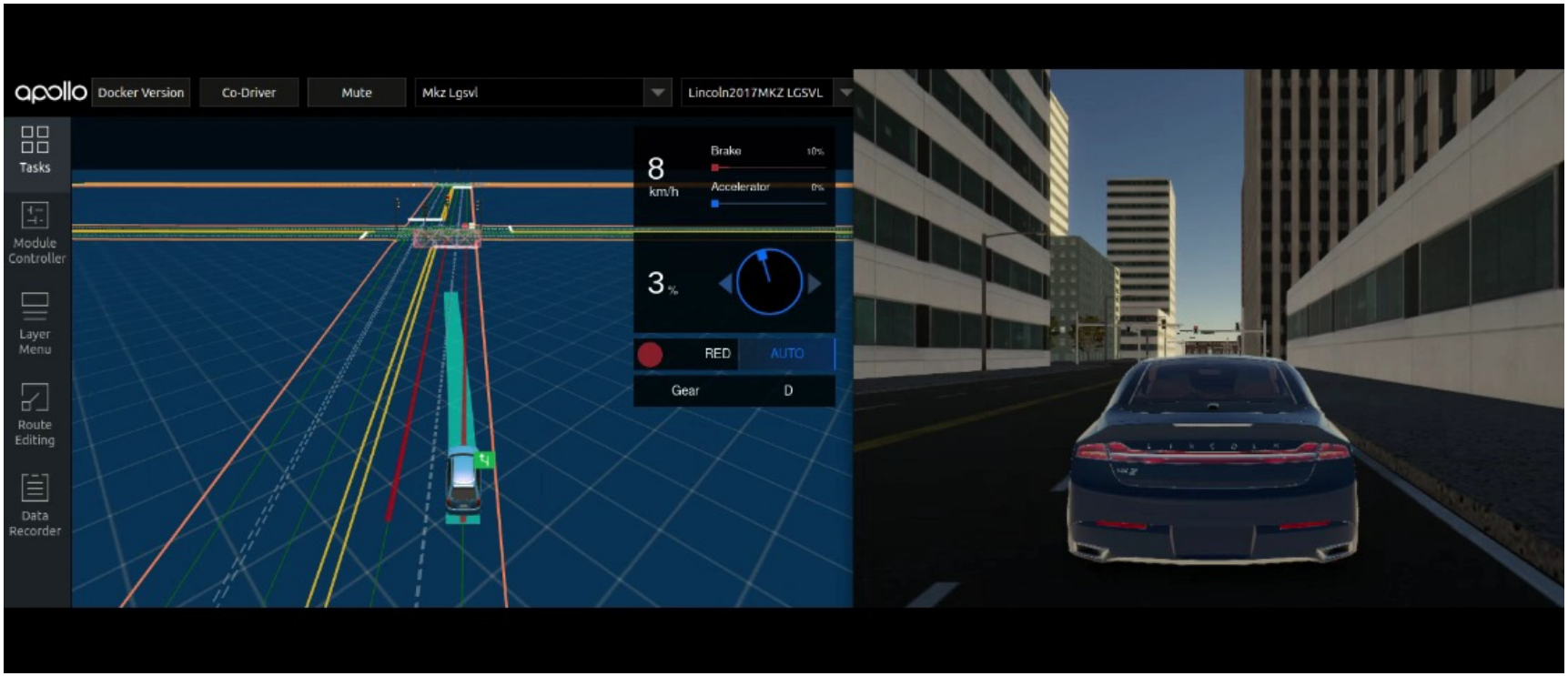
- As a result, a new standard has recently emerged
  - ISO 21448: Safety Of The Intended Functionality (SOTIF)
  - ISO 34502: Road vehicles — Test scenarios for automated driving systems — Scenario based safety evaluation framework

Immobile in Intersection

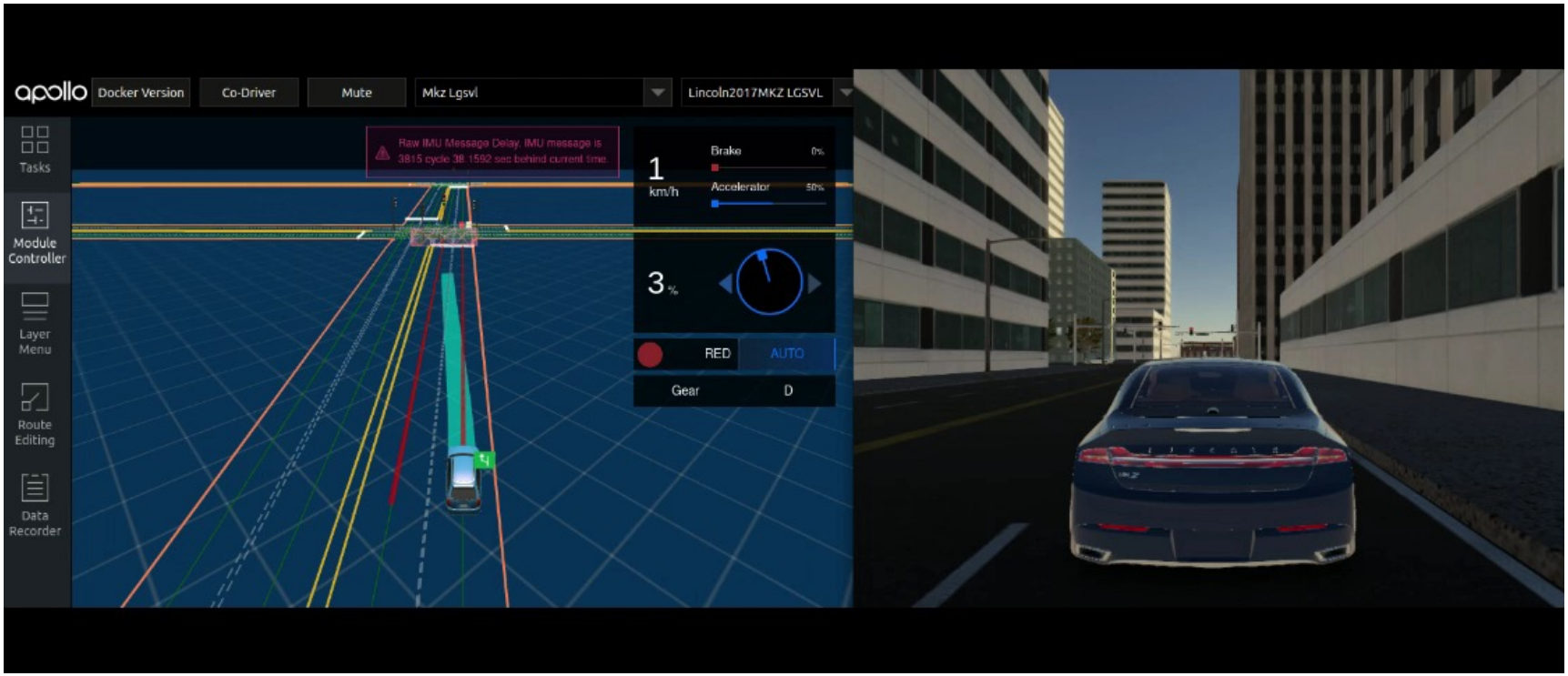
Immobile in Intersection

Sensor fusion bug (Normal Driving)

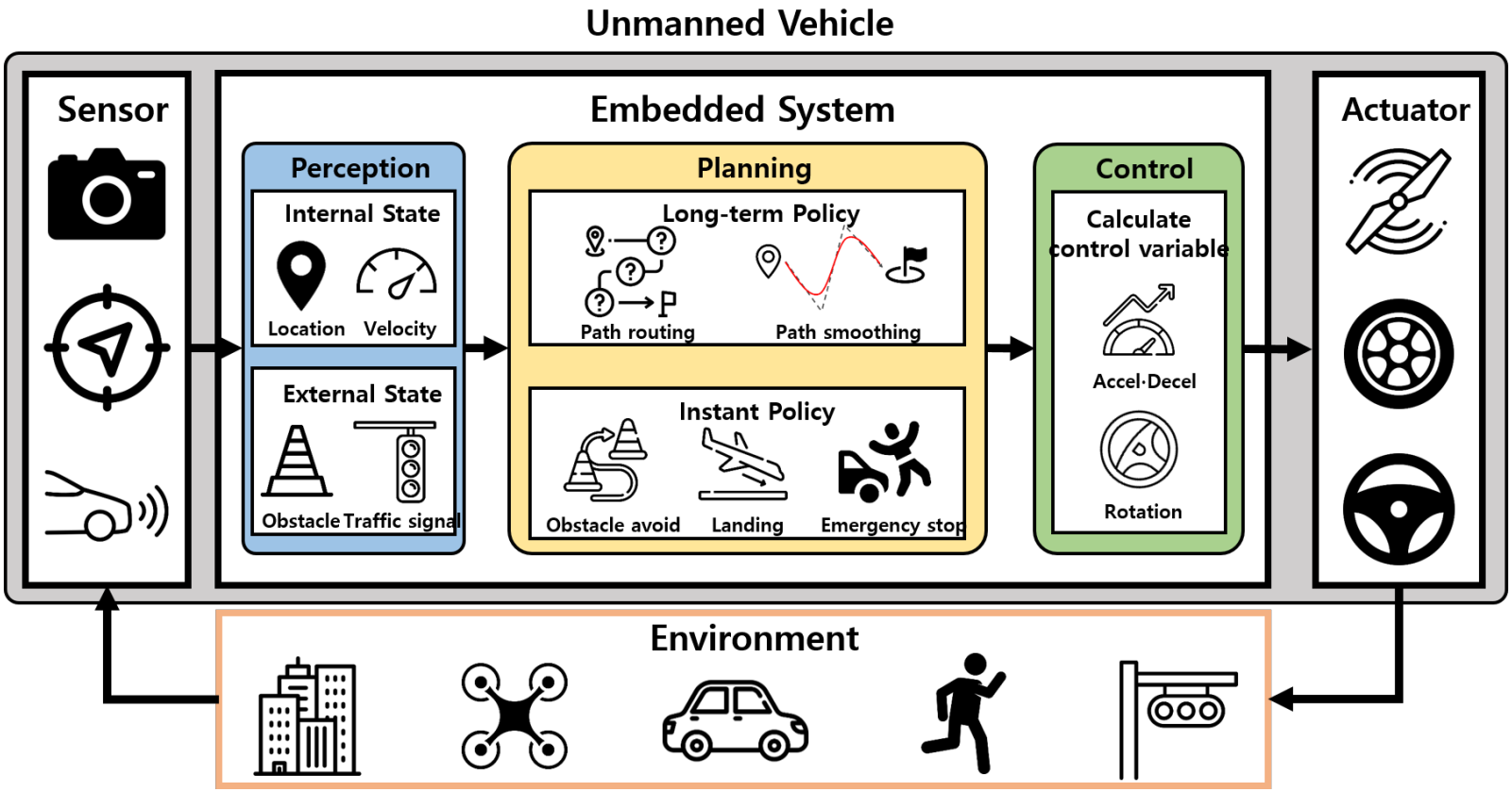
Sensor fusion bug (Night)



Sensor fusion bug (Rain+Lidar)



Unmanned Vehicle



Conclusion

- Unmanned ➔ Automatic ➔ AI?
- Physical attacks?

- What attacks should be in scope?
- RL under adversarial environment?
- Self-driving vehicle may be much more difficult
  ➔ Incremental deployment?

Questions?

- Yongdae Kim
  - email: yongdaek@kaist.ac.kr
  - Home: http://syssec.kaist.ac.kr/~yongdaek
  - Facebook: https://www.facebook.com/y0ngdaek
  - Twitter: https://twitter.com/yongdaek
  - Google “Yongdae Kim”