Lecture 4: Safety III

Professor Katie Driggs-Campbell

January 25, 2024

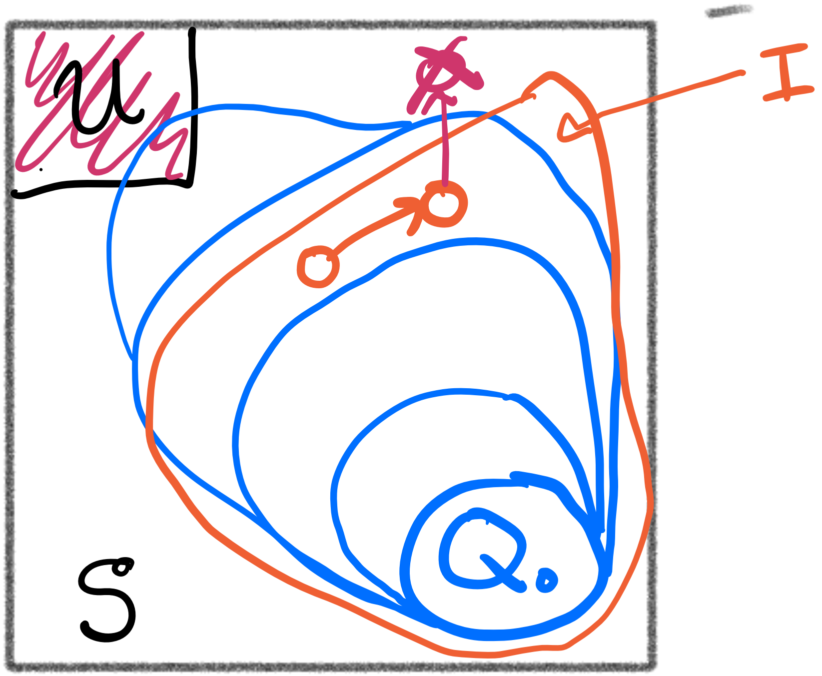
ECE484: Principles of Safe Autonomy

Videos courtesy of Tianchen Ji

Administrivia

- Lab starts this week – will introduce MP0

Core Idea of Inductive Invariants



Adding more information

timer := 0

while → if $x_2 - x_1 < d_s$

  if $v_1 > a_b$

    → $v_1 := v_1 - a_b$ (A)

    timer := timer + 1

  else $v_1 = 0$ (B)

else $v_1 := v_1$ (C)

$x_1 := x_1 + v_1$

$x_2 := x_2 + v_2$

end

I_3: $\text{timer} \le \frac{v_{10} - v_1}{a_b}$

(1) $q_0.\text{timer} = 0 \le \frac{v_{10} - q_0.v_1}{a_b}$ (v_{10}, ≥ 0)

(2) $q \in I_3 \Rightarrow q' \in I_3$

consider 3 cases

A, B, C

Three Cases to Consider: (1) A

$$q'.timer = q.timer + 1$$

$$\leq \frac{v_{10} - q.v_1}{a_b} + 1 = \frac{v_{10} - (q'.v_1 + a_b)}{a_b} + 1$$

$$\leq \frac{v_{10} - q'.v_1}{a_b} \quad \checkmark$$

Three Cases to Consider: (2) (B)

$$q'.timer = q.timer \leq \frac{v_{10} - \boxed{q.v_1}}{a_b} \leq \frac{v_{10} + 0}{a_b} \checkmark$$

($q.v_1 \geq 0$)

Three Cases to Consider: (3)

$$q'.timer = q.timer \leq \frac{v_{10} - q.v_1}{a_b}$$

$$\leq \frac{v_{10} - q'.v_1}{a_b} \quad \checkmark$$

$$I_3 : timer \leq \frac{v_{10} - v_1}{a_b} \text{ and } v_1 \geq 0$$

$$\Rightarrow timer \leq \frac{v_{10}}{a_b}$$

Showing Safety with a Timer

- Goal: show $x_2 - x_1 > 0$
- Maximum distance traveled by car 1 after detection:

when $x_2 - x_1 < d_s$

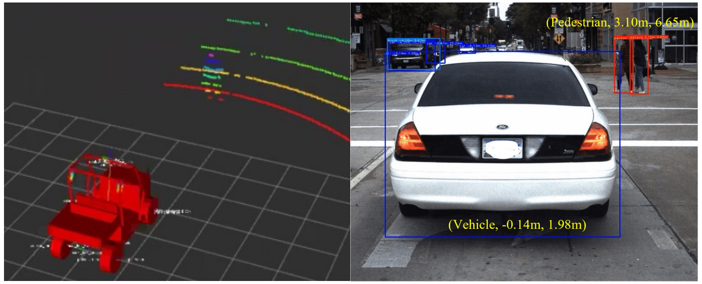
$d_{max} \le v_{10} \cdot timer \le v_{10}^2 / a_b$

if $d_s > v_{10}^2 / a_b$ and $v_2 \ge 0$

then $I_3 \Rightarrow S: x_2 > x_1$

Baked-in Assumptions (1)

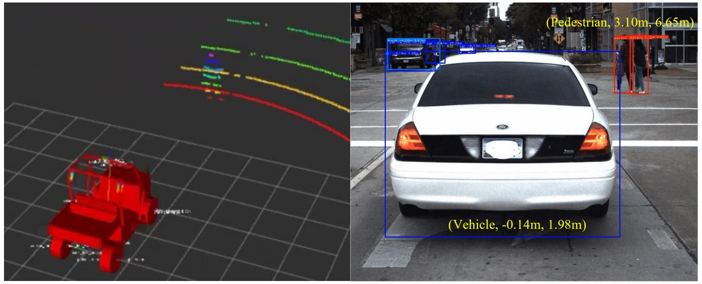
- Perception.
  - Sensor detects obstacle **iff** distance $d \leq D_{sense}$
  - How to model vision errors?



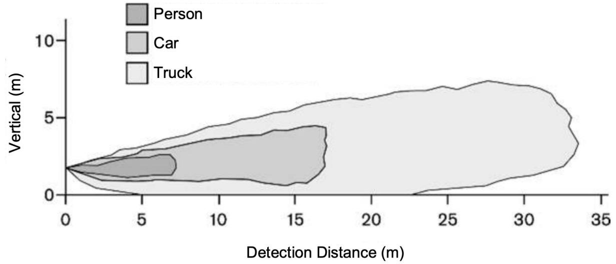
1.2.1.2 Vertical Detection Area

Baked-in Assumptions (1)

- Perception.
  - Sensor detects obstacle **iff** distance $d \leq D_{sense}$
  - How to model vision errors?
- Pedestrian Behaviors.
  - Pedestrian is assumed to be moving with constant velocity from initial position

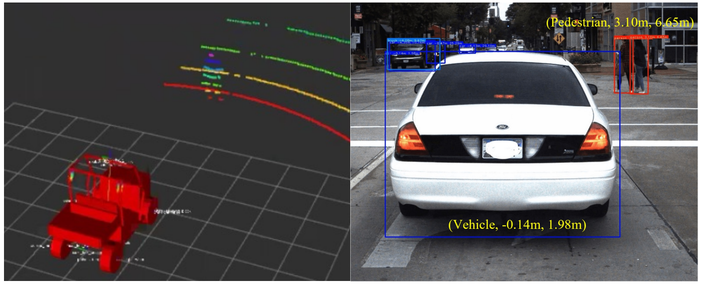


1.2.1.2 Vertical Detection Area



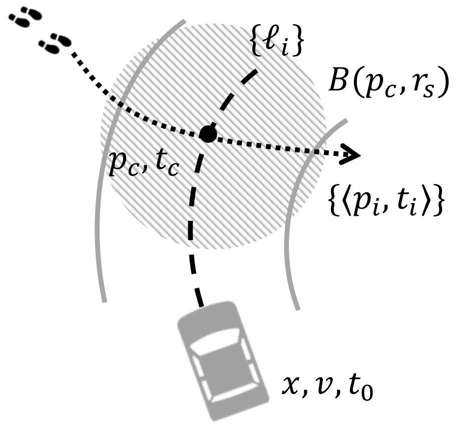
Baked-in Assumptions (1)

- Perception.
  - Sensor detects obstacle **iff** distance $d \leq D_{sense}$
  - How to model vision errors?
- Pedestrian Behaviors.
  - Pedestrian is assumed to be moving with constant velocity from initial position
- No sensing-computation-actuation delay.
  - The time step in which $d \leq D_{sense}$ is true is exactly when the velocity starts to decrease



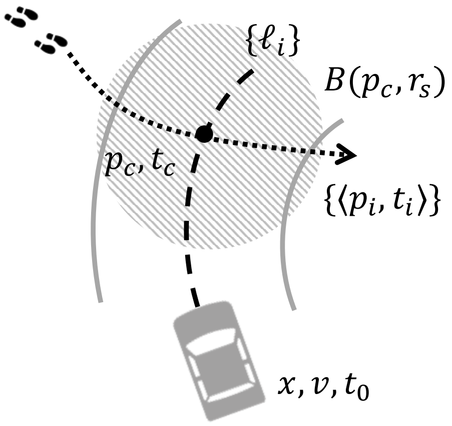
1.2.1.2 Vertical Detection Area

Baked-in Assumptions (2)



- Mechanical or Dynamical assumptions
  - Vehicle and pedestrian moving in 1-D lane.
  - Does not go backwards.
  - Perfect discrete kinematic model for velocity and acceleration.

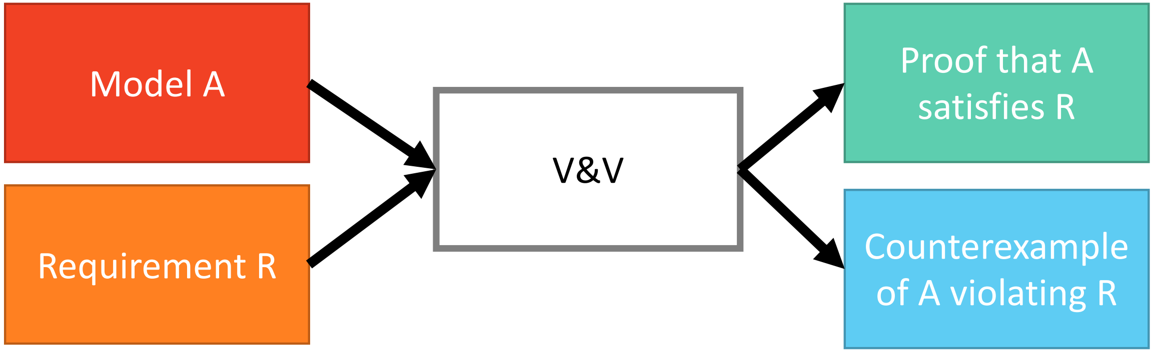
Baked-in Assumptions (2)



- Mechanical or Dynamical assumptions
  - Vehicle and pedestrian moving in 1-D lane.
  - Does not go backwards.
  - Perfect discrete kinematic model for velocity and acceleration.
- Nature of time
  - Discrete steps. Each execution of the above function models advancement of time by 1 step. If 1 step = 1 second, $x_1(t+1) = x_1(t) + v_1(t).1$
  - Atomic steps. 1 step = complete (atomic) execution of the program.
    - We cannot directly talk about the states visited after partial execution of program

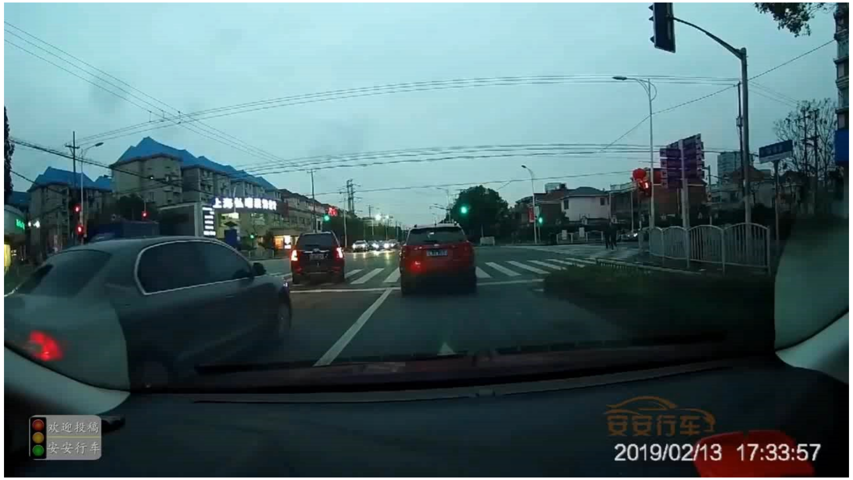
Remarks and Takeaway

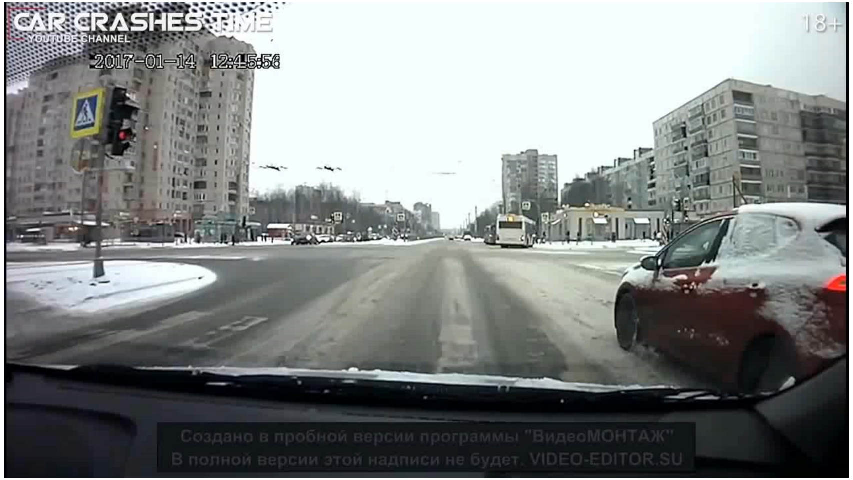
- The proof by induction shows a property of ***all behaviors of our model***
- The proof is conceptually simple, but can quickly get tedious and error prone
  - Verification and Validation tools like Z3, Dafny, PVS, CoQ, AST, MC2, automate this



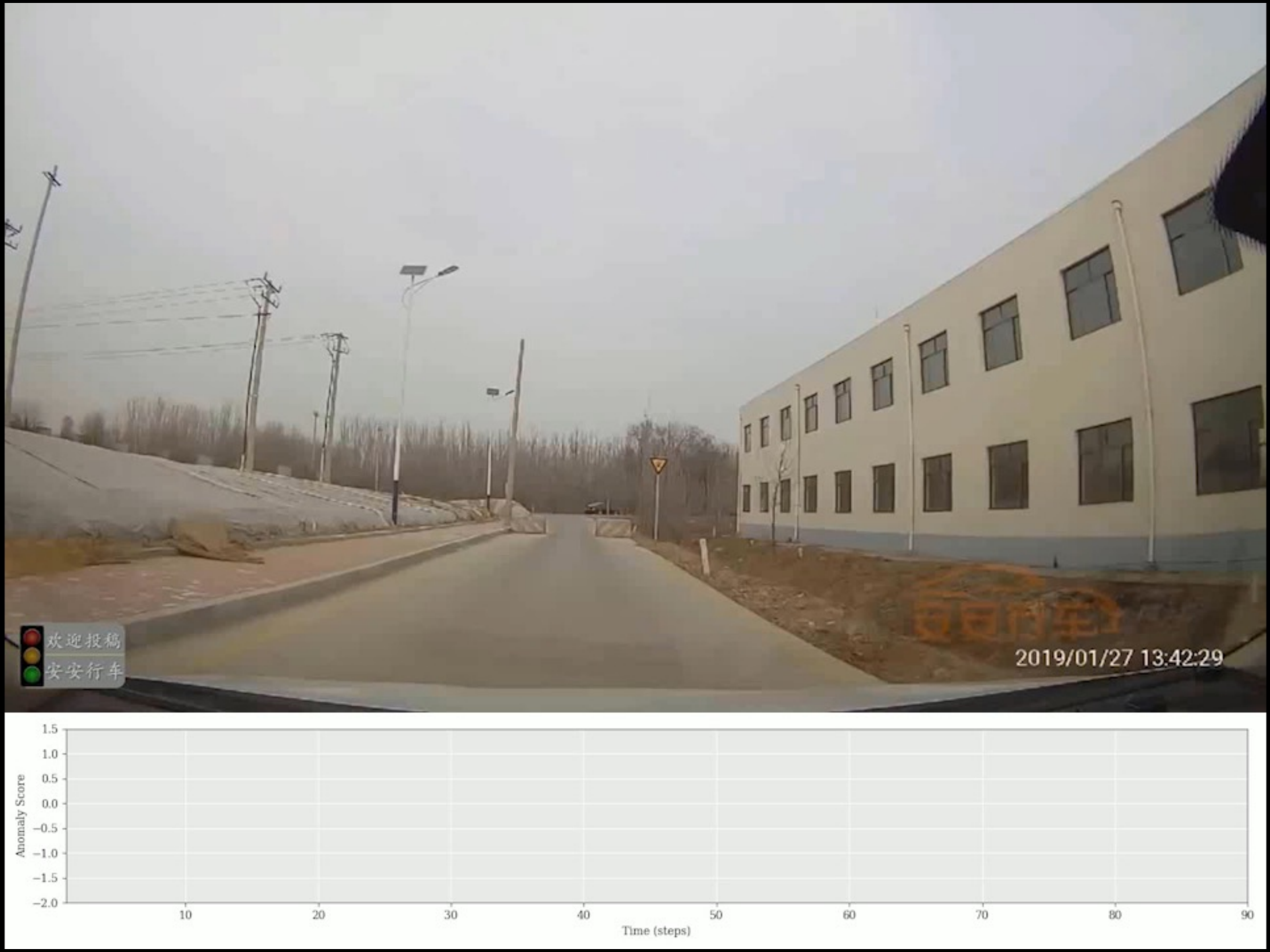
Rare Events and Safety Proxies

Anomalies in Driving Scenes

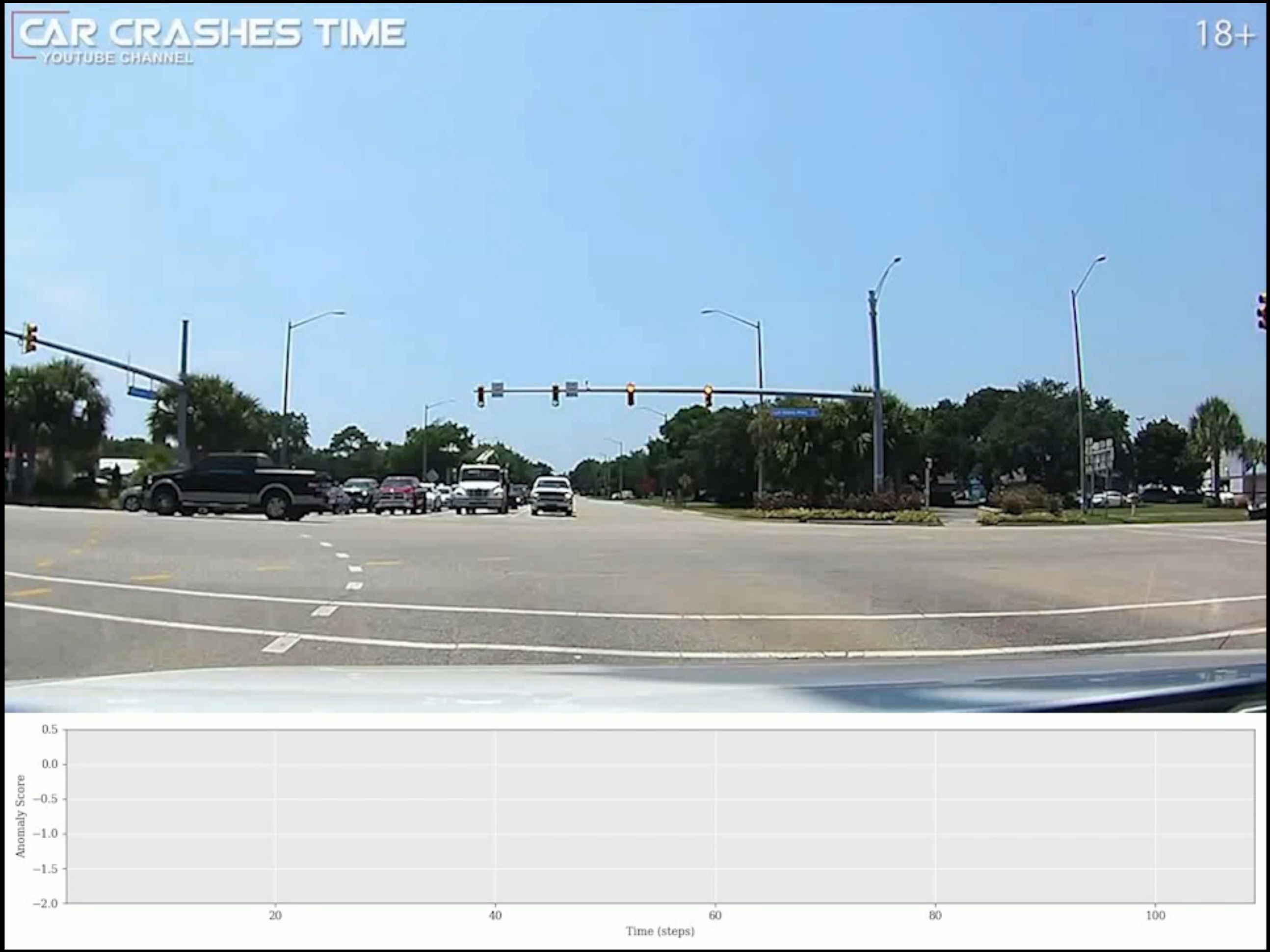




On-Road Anomaly Detection



On-Road Anomaly Detection

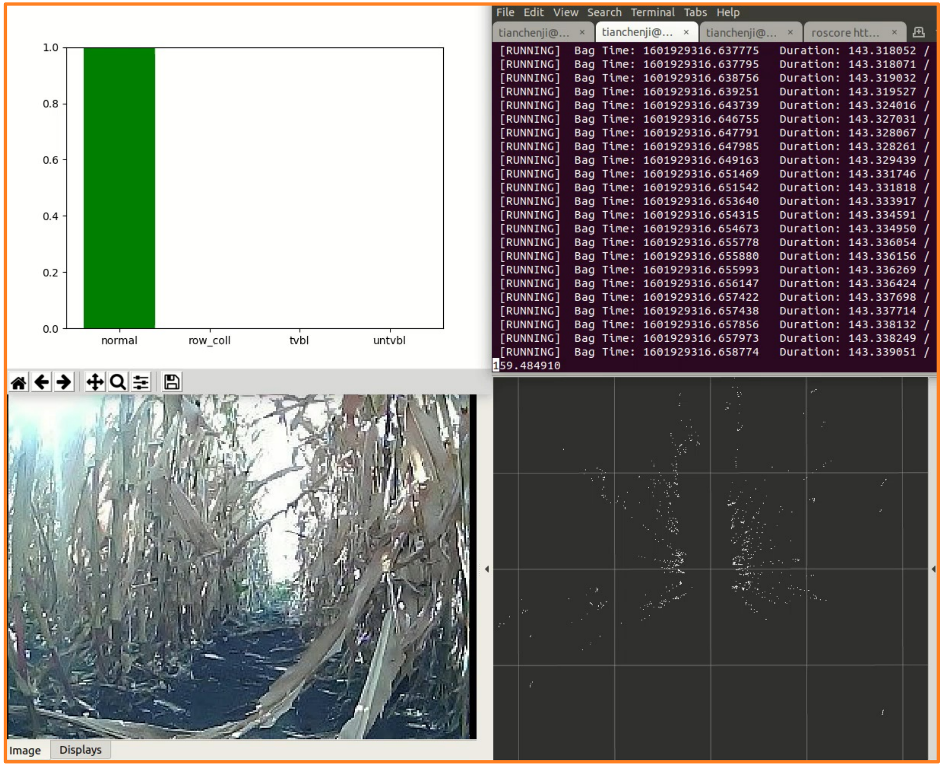


Anomalies in Field Environments



Reactive Anomaly Detection

Reactive Anomaly Detection



Proactive Anomaly Detection

Summary

- Invariant trick can give a shortcut for proving safety ☺
  - The invariant I may contain important information about conserved quantities and may also tell us why the system is safe
  - However, often requires guessing and checking and a lot of engineering effort
- Online Monitoring is another key component to safe systems
  - Anomaly detection is a reasonably proxy for safety, if you don’t mind false positives
- Next week: starting perception