Lecture 2: Safety I

Professor Katie Driggs-Campbell

January 17, 2024

ECE484: Principles of Safe Autonomy

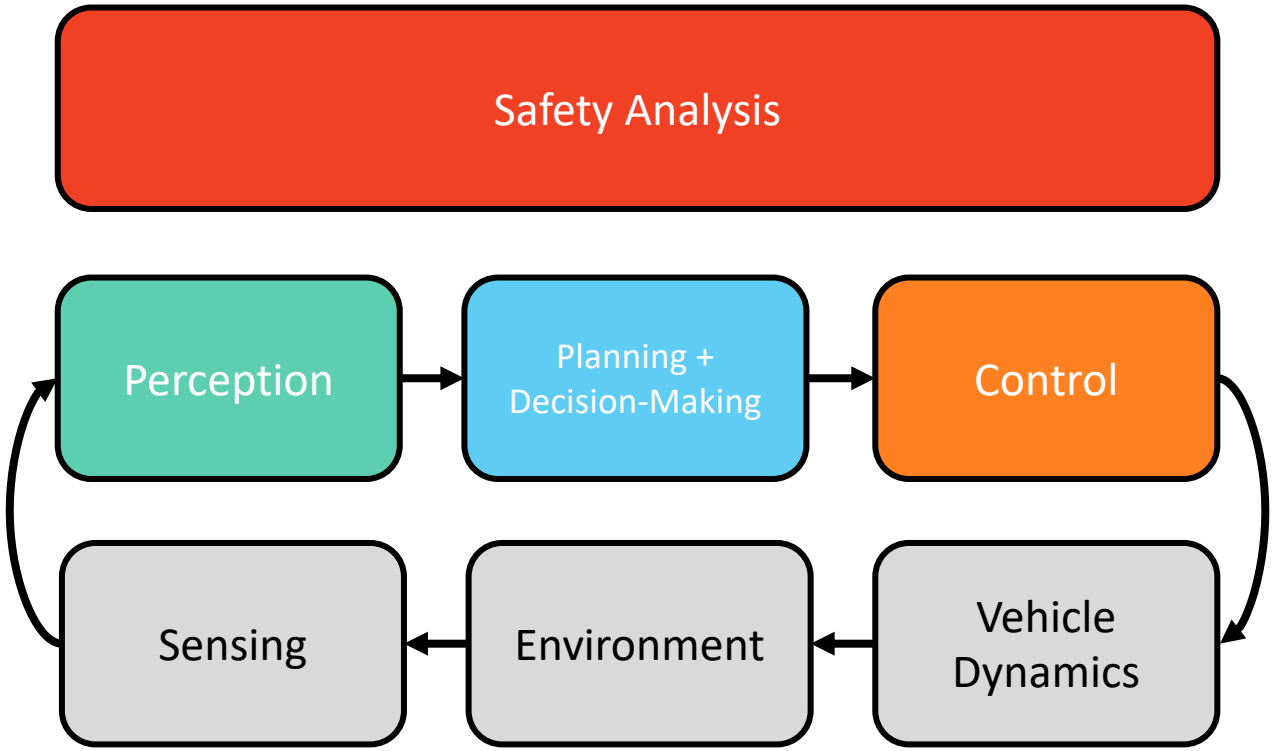
Administrivia

- Re course registration: Please sign up for lab sections!
- Canvas and campuswire setup – let me know if you do not have access
- We will have pop quizzes throughout the semester and one exam (4/18)

Today's Lecture

- Quick background on models
- Introducing automata and safety verification

Autonomous GEM Vehicle



How to assess safety?

1. Create a *model* of the autonomous system
   - What are the inputs and outputs to the system?
   - What are the expectations on behaviors?
   - No model is perfect – some models are useful!
   - What are the implicit and explicit biases in your system?

How to assess safety?

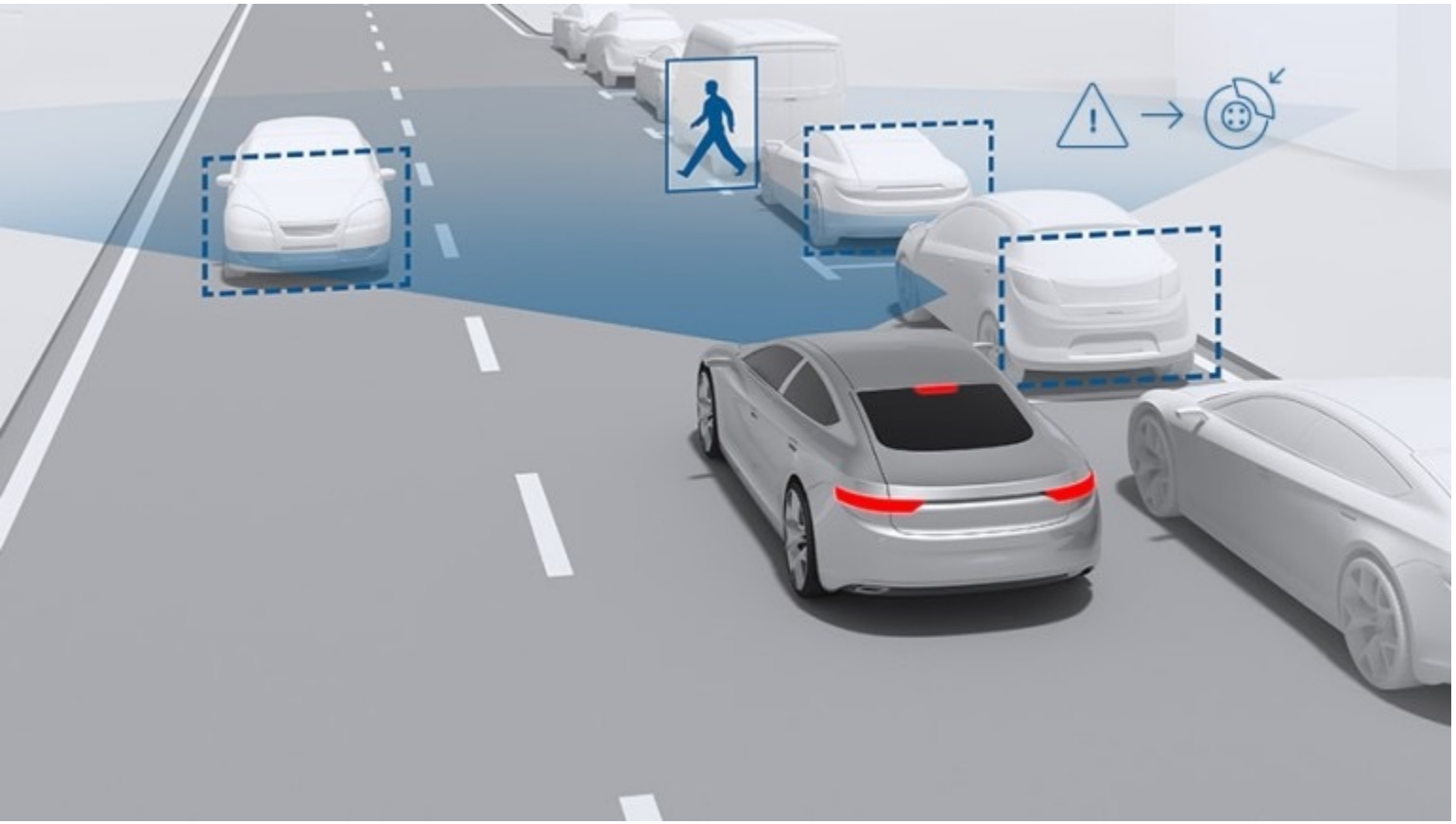
1. Create a *model* of the autonomous system
   - What are the inputs and outputs to the system?
   - What are the expectations on behaviors?
   - No model is perfect – some models are useful!
   - What are the implicit and explicit biases in your system?
2. Identify the *requirements* and *assumptions*
   - What parts of the model are available for observation/analysis?

How to assess safety?

1. Create a *model* of the autonomous system
   - What are the inputs and outputs to the system?
   - What are the expectations on behaviors?
   - No model is perfect – some models are useful!
   - What are the implicit and explicit biases in your system?
2. Identify the *requirements* and *assumptions*
   - What parts of the model are available for observation/analysis?
3. Analyze model to show that it meets the requirements under the assumptions

What are some safety requirements for AVs? What are your design considerations?

Emergency Braking for Pedestrians




LiveLeak

Simple State Machines and Automaton

- Definition: A state machine or an automaton is defined as:

Cruise Control Example

Deterministic Automaton

Example: Emergency Braking System (1)

Example: Emergency Braking System (2)

Executions and Behaviors

- Definition: an execution is a particular behavior or trajectory of an automaton

Safety Requirements

We want to express our safety requirements as:

1. A formula involving state variables
2. A subset of Q

The Safety Verification Problem

Reachability and the Post operator

Summary

- Start thinking about forming your team and decide project track
  - Sign-up to be member of IRL if interested in hardware projects
- All models are wrong, but some are useful!
- Think about how to define your safety requirements formally
- Automata provide us simple models for safety verification
- Next time: inductive invariants to prove safety for simple programs!