Principles of Safe Autonomy
ECE 484 Lecture 2: System Safety

Professors: Sayan Mitra

Graduate Teaching Assistants: Yangge Li and Minghao Jiang

Welcome from Safe Autonomy team!

Professor

Sayan Mitra (mitras) (CSL 266)

TAs

Tianchen Ji (tj12)

Pranav Sriram (psriram2)

Lab assistants

Haoyuan You (hy19)

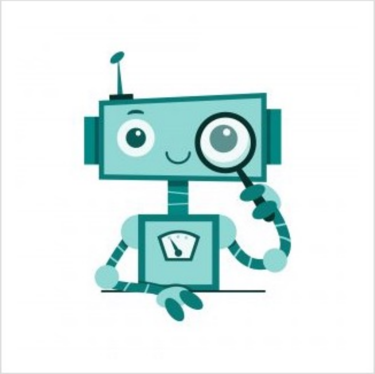
Ninghan Zhong (innghan2)

Sayan Mitra (Instructor)

Tianchen Ji (tj12)

Pranav Sriram (psriram2)

Ninghan Zhong (ninghan2)



Haoyuan You (hy19)

Last time on how to assure safety of an autonomous system

"Testing can be used to show the presence of bugs, but never to show their absence!'' --- Edsger W. Dijkstra

Because there are infinitely many *executions* and we can only test finitely many of those in any testing algorithm

In a probabilistic sense also, purely using data to gain safety assurance is not practical

Data required to guarantee a probability of 10^{-9} fatality per hour of driving is proportional to its inverse, 10^9 hours, 30 billion miles

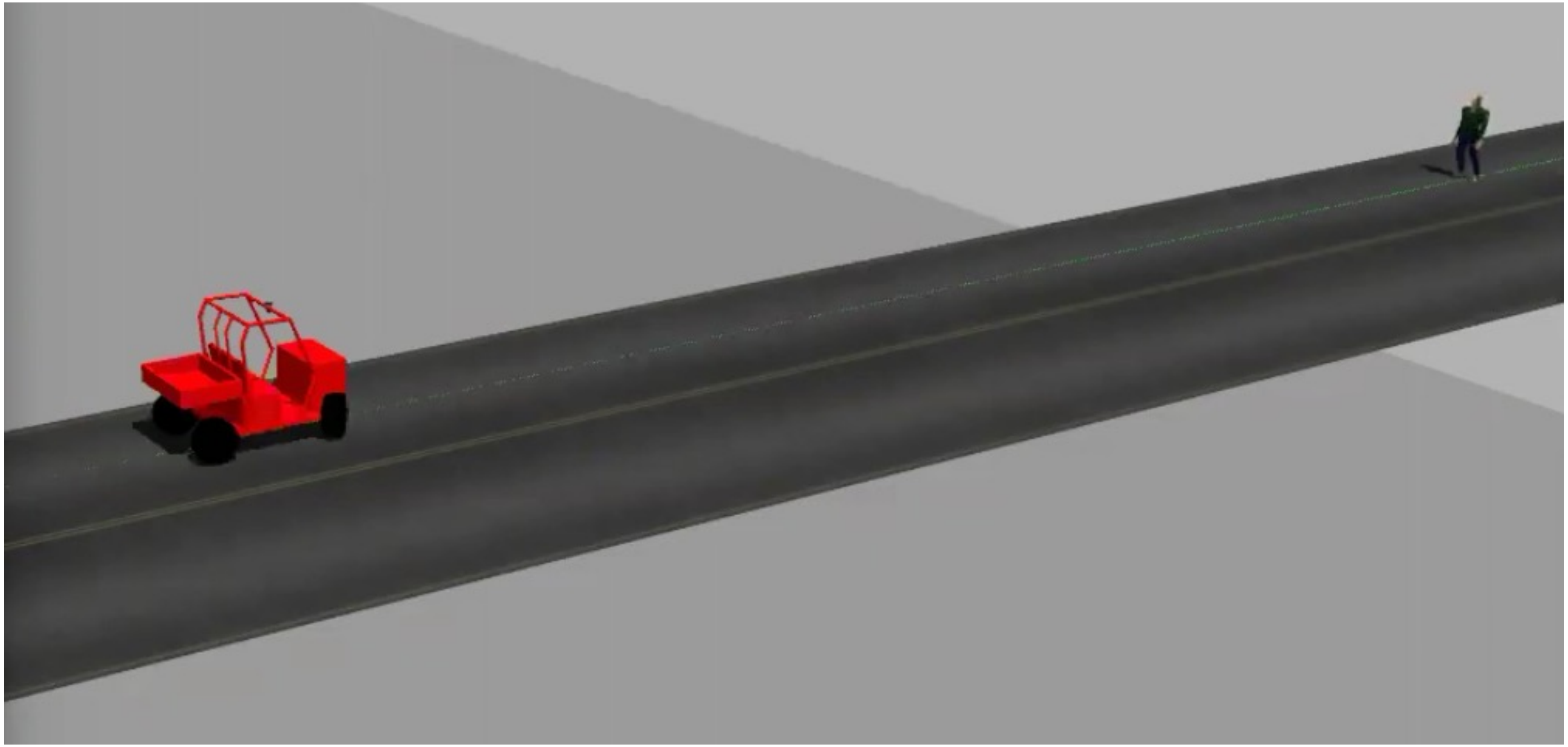
To learn or extrapolate about all---infinitely many---executions from a finite sampling of executions, we need to make some assumptions about the system. A collection of these assumptions defines a ***model***

On a Formal Model of Safe and Scalable Self-driving Cars by Shai Shalev-Shwartz, Shaked Shammah, Amnon Shashua, 2017 (Responsibility Sensitive Safety)

Roadmap

- A simple class of models: *automata*.
- What are executions of automata: sequence of states
- What are *requirements*?
- *Reachable states*, why we care to compute and why that can be hard
- *Invariants* as approximations of reachable states

Model (switch to notes)



A “simple” safety scenario

A car moving down a straight road has to detect any pedestrian in front of it and stop before it collides.

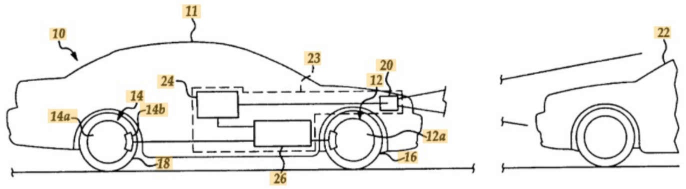
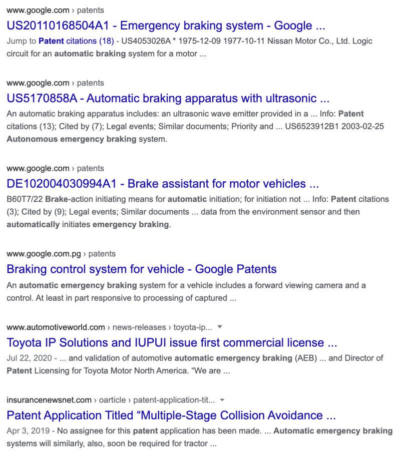


Figure 1



www.google.com › patents
US20110168504A1 - Emergency braking system - Google ...
Jump to **Patent** citations (18) - US4053026A * 1975-12-09 1977-10-11 Nissan Motor Co., Ltd. Logic circuit for an **automatic braking** system for a motor ...

www.google.com › patents
US5170858A - Automatic braking apparatus with ultrasonic ...
An automatic braking apparatus includes: an ultrasonic wave emitter provided in a ... Info: **Patent** citations (13); Cited by (7); Legal events; Similar documents; Priority and ... US6523912B1 2003-02-25 **Autonomous emergency braking** system.

www.google.com › patents
DE102004030994A1 - Brake assistant for motor vehicles ...
B60T7/22 **Brake**-action initiating means for **automatic** initiation; for initiation not ... Info: **Patent** citations (3); Cited by (9); Legal events; Similar documents ... data from the environment sensor and then **automatically** initiates **emergency braking**.

www.google.com.pg › patents
Braking control system for vehicle - Google Patents
An **automatic emergency braking** system for a vehicle includes a forward viewing camera and a control. At least in part responsive to processing of captured ...

www.automotiveworld.com › news-releases › toyota-ip...
Toyota IP Solutions and IUPUI issue first commercial license ...
Jul 22, 2020 - ... and validation of automotive **automatic emergency braking** (AEB) ... and Director of **Patent** Licensing for Toyota Motor North America. “We are ...

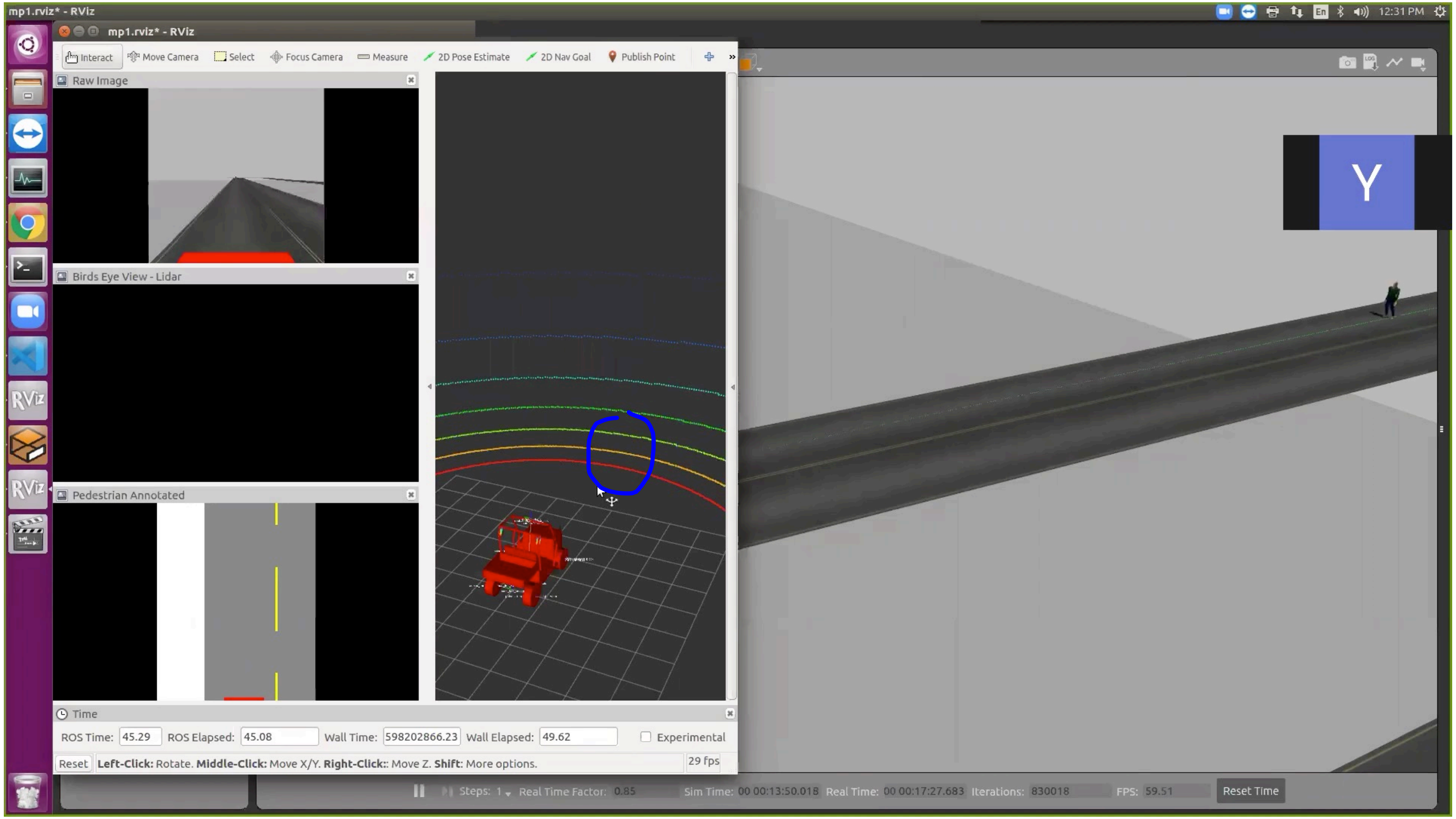
insurancenewsnet.com › oarticle › patent-application-tit...
Patent Application Titled “Multiple-Stage Collision Avoidance ...
Apr 3, 2019 - No assignee for this **patent** application has been made. ... **Automatic emergency braking** systems will similarly, also, soon be required for tractor ...

Automatic Emergency Braking

Not a trivial requirement

"simple" ≠ Easy

MP0: Simulate model for testing



“All models are wrong, some are useful.”

Wrong and useless models

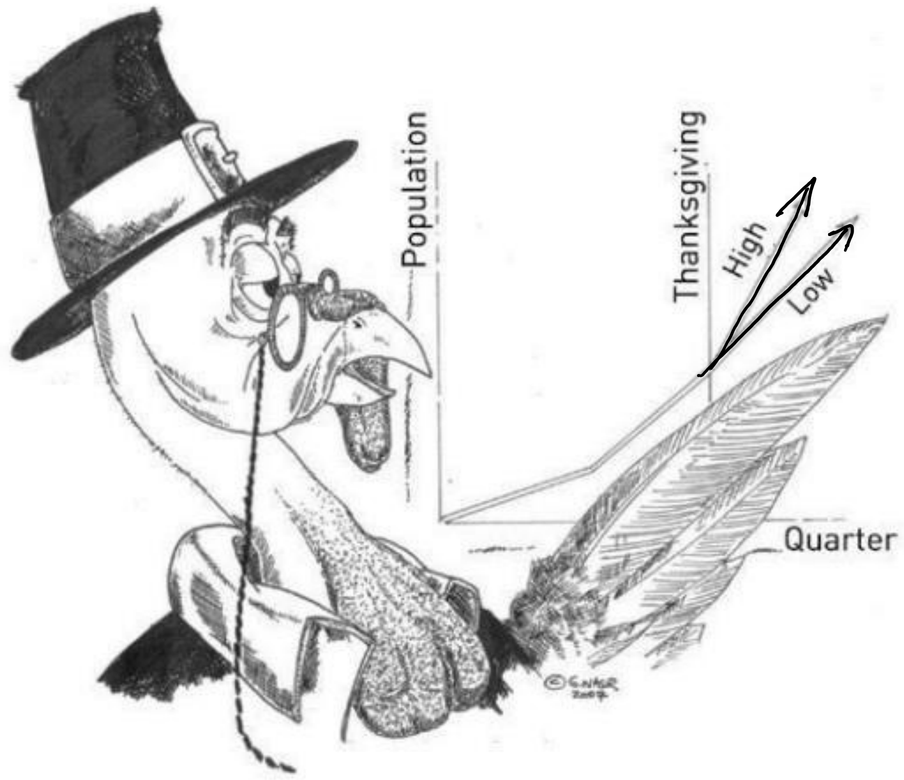
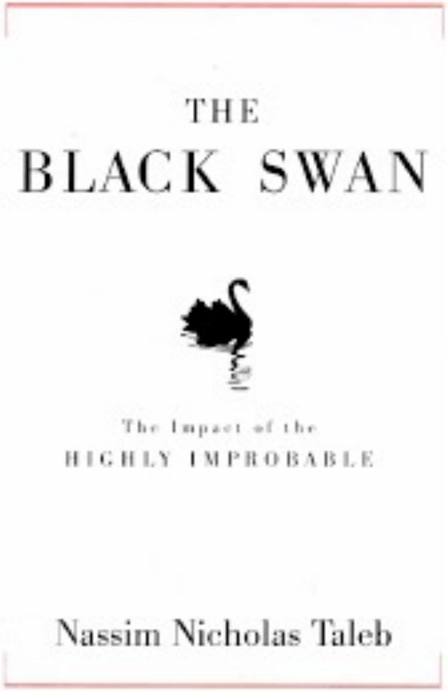
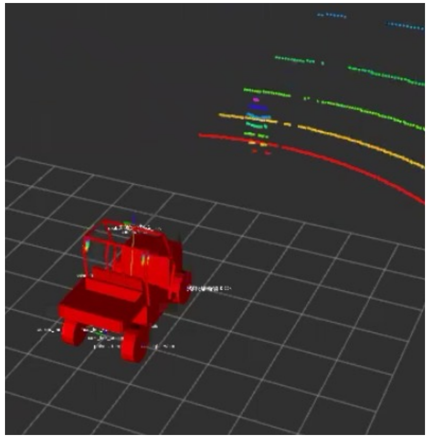


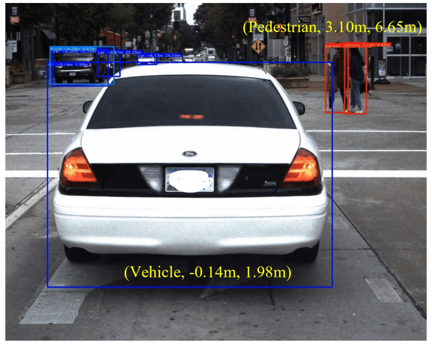
FIGURE 4. A turkey using "evidence"; unaware of Thanksgiving, it is making "rigorous" future projections based on the past. Credit: George Nasr

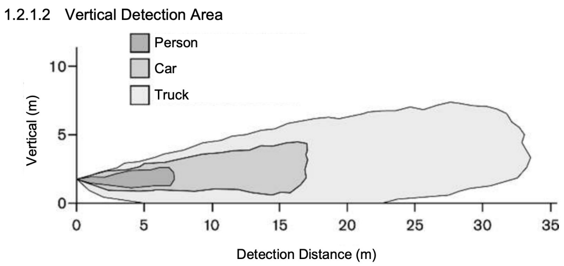


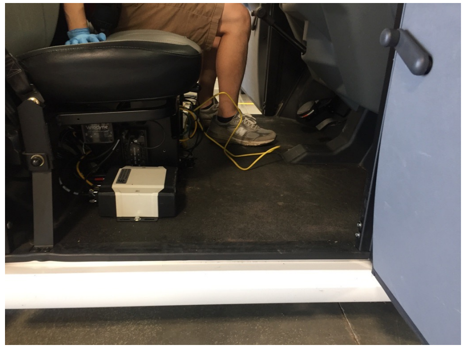
Baked-in Assumptions in our example

- Perception.
  - Sensor detects obstacle **iff** distance $d \leq D_{sense}$
  - No false positives, negatives, probabilities
  - Pedestrian is known to be moving with constant velocity from initial position. This will be used in the safety analysis, but not in the vehicle's automatic braking algorithm
- No sensing-computation-actuation delay.
  - The time step in which $d \leq D_{sense}$ becomes smaller is exactly when the velocity starts to decrease

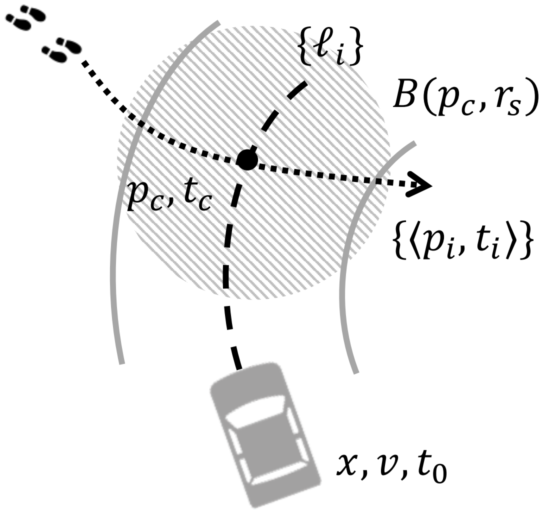








Baked-in Assumptions (continued)



- 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, $x_1(t+1) = x_1(t) + v_1(t).1$
    - We cannot talk about what happens between [t, 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

Summary

- Absolute safety checking boils down to showing that none of the executions of the automaton reaches an unsafe set U
- To reason about all executions of we have to work with infinite sets of states
- One way to compute infinite sets is using the Post operator
- But, computing all executions for unbounded time can be hard
- If we can guess an invariant satisfying conditions of Proposition 1.1, that can give a shortcut for proving safety
- The inavariant may contain important information about conserved quantities, and thus, may tell us why the system is safe, and not just that it is so
- Mind the gap between model and reality
- Next. Application of invariants in braking example