Autonomous Vehicle Safety Technical and Social Issues

WAISE, Sept. 18, 2018

Prof. Philip Koopman

Carnegie Mellon University

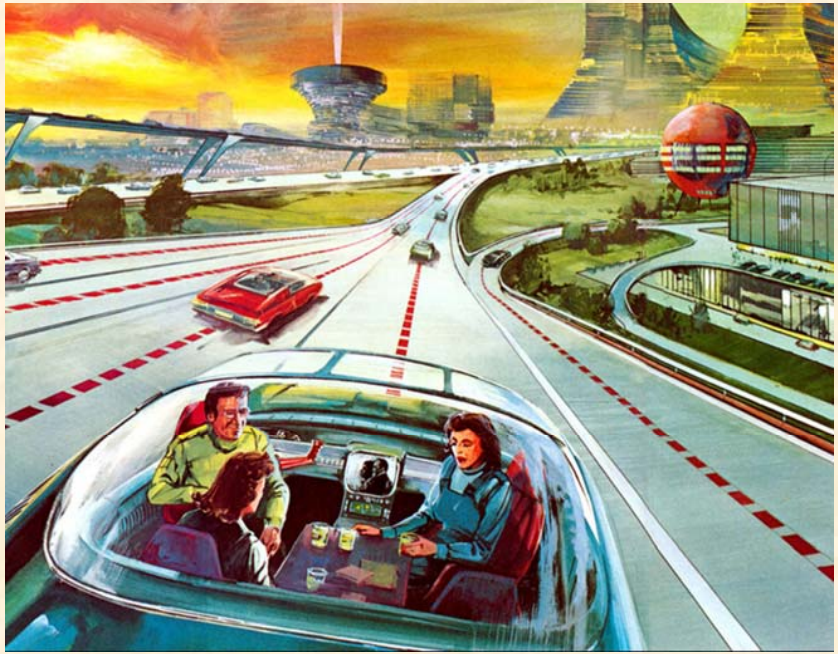
Electrical & Computer ENGINEERING

Edge Case Research

Overview

Carnegie Mellon University

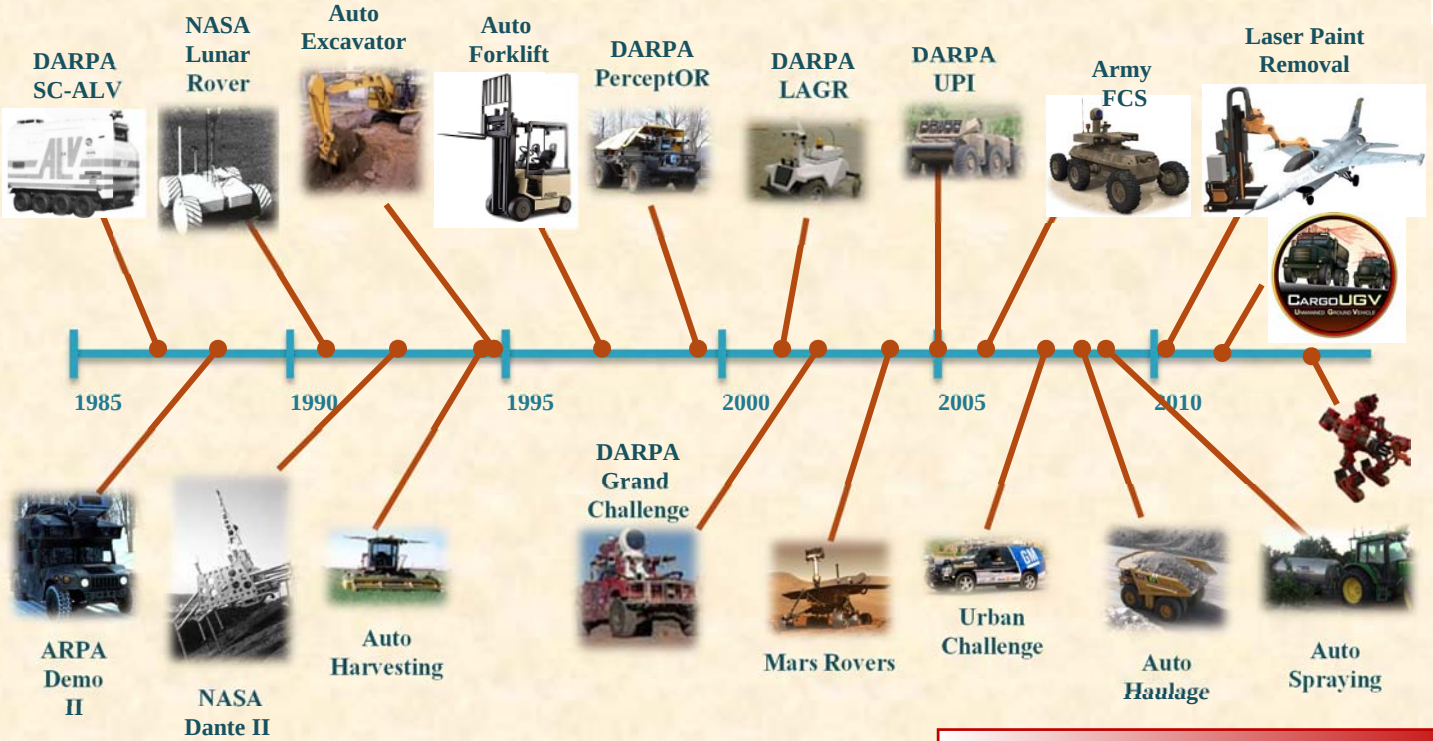
- Control & Planning safety
- Perception safety
- Edge cases
- Some hard questions about AV safety



[General Motors]

NREC: 30+ Years Of Cool Robots

NATIONAL ROBOTICS NREC ENGINEERING CENTER



Software
Safety

Carnegie Mellon University Faculty, staff, students
Off-campus Robotics Institute facility

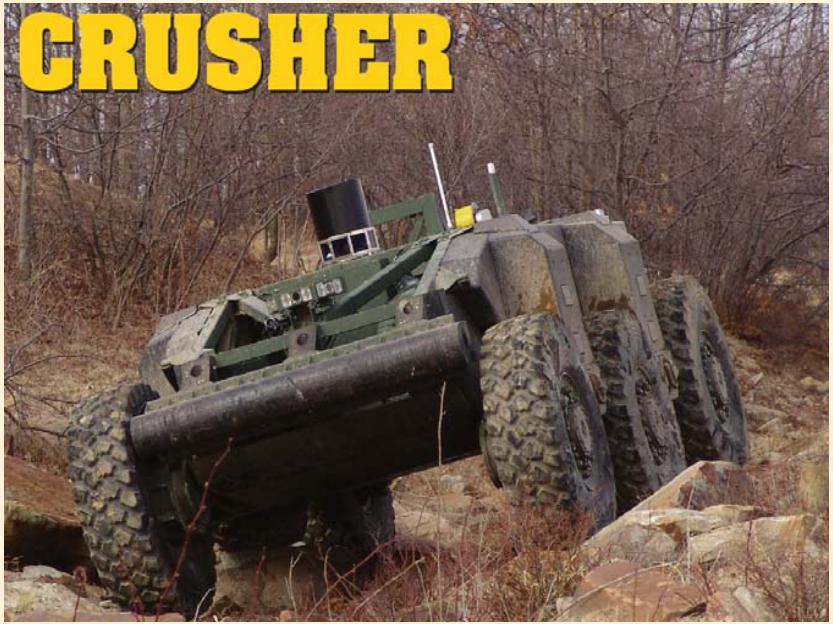
Researchers evaluated 150 bugs from 11 distinct projects over 4 years [ICSE 2018]

From "RIOT Expanded Technical Brief, NAVAIR Public Release- 2016-842 'Approved for Public Release; distribution is unlimited'.

Before Autonomy Software Safety

Carnegie Mellon University

- The **Big Red Button** era



APD (Autonomous Platform Demonstrator)
How did we make this scenario safe?

NATIONAL ROBOTICS ENGINEERING CENTER

TARGET GVW: 8,500 kg

TARGET SPEED: 80 km/hr

Approved for Public Release. TACOM Case #20247 Date: 07 OCT 2009

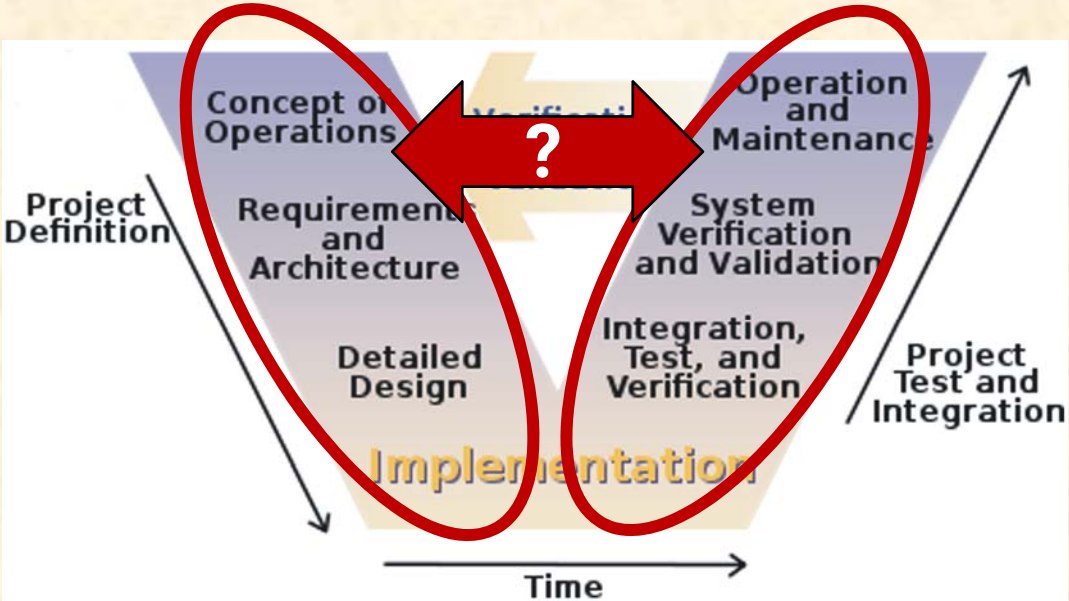
Traditional Validation Meets Machine Learning

Carnegie Mellon University

- **Use traditional software safety where you can**

..BUT..

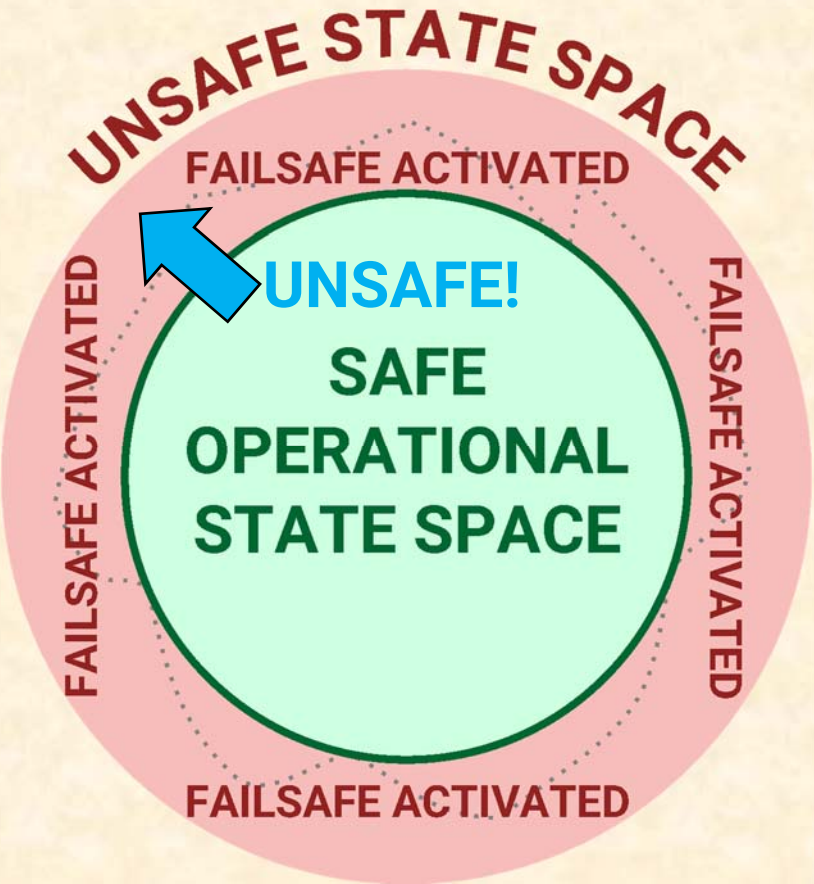
- **Machine Learning (inductive training)**
  - No requirements
    - Training data is difficult to validate
  - No design insight
    - Generally inscrutable
    - Prone to over-fitting/gaming



Safety Envelope Approach to ML Deployment

Carnegie Mellon University

- **Specify unsafe regions**
- **Specify safe regions**
  - Under-approximate to simplify
- **Trigger system safety response upon transition to unsafe region**



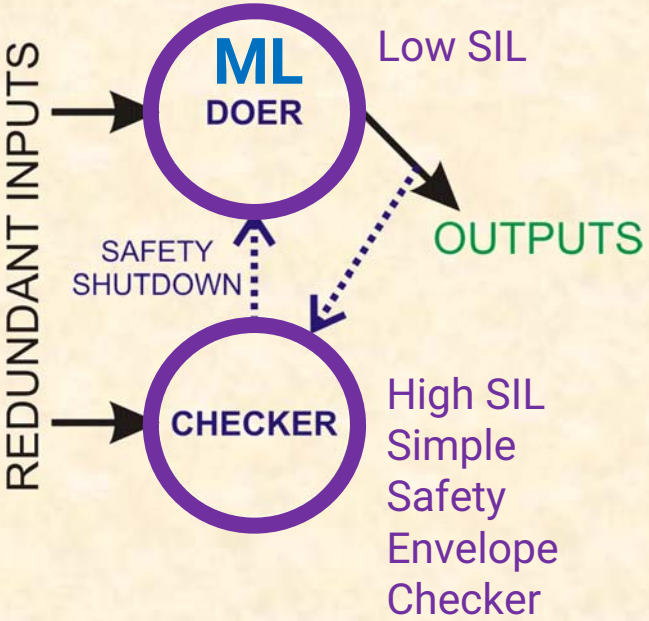
Architecting A Safety Envelope System

Carnegie Mellon University

- **"Doer" subsystem**
  - Implements normal, untrusted functionality
- **"Checker" subsystem – Traditional SW**
  - Implements failsafes (safety functions)
- **Checker entirely responsible for safety**
  - Doer can be at low Safety Integrity Level
  - Checker must be at higher SIL

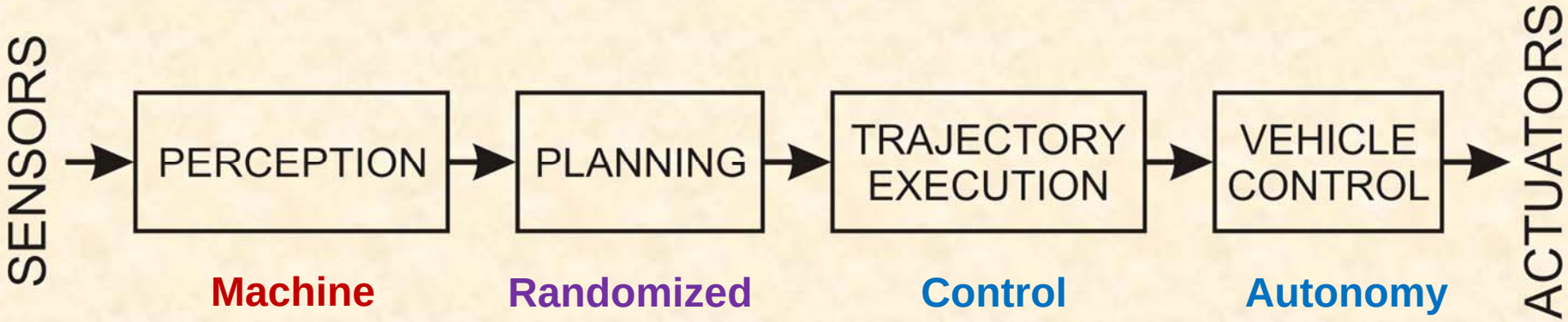
(Also known as a "safety bag" approach)

Doer/Checker Pair



Validating an Autonomous Vehicle Pipeline

Carnegie Mellon University



Machine Learning Based Approaches

➔ ???

Randomized & Heuristic Algorithms

➔ Run-Time Safety Envelopes

➔ Doer/Checker Architecture

Control Systems

➔ Control Software Validation

➔ Doer/Checker Architecture

Autonomy Interface To Vehicle

➔ Traditional Software Validation

Perception presents a uniquely difficult assurance challenge

Brute Force Road Testing

Carnegie Mellon University

- **If 100M miles/critical mishap…**
  - Test 3x–10x longer than mishap rate
    ➔ Need 1 Billion miles of testing

- **That's ~25 round trips on every road in the world**
  - With fewer than 10 critical mishaps

…

WolframAlpha computational knowledge engine.

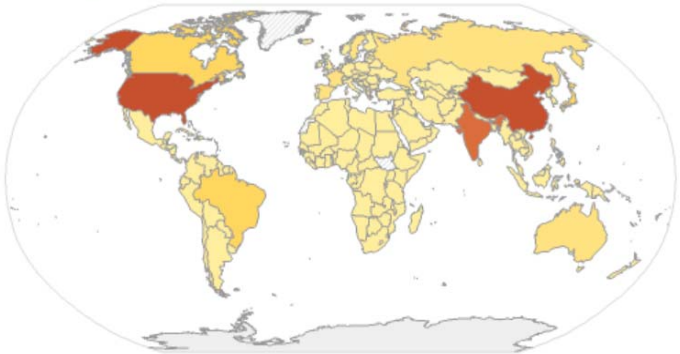
miles of roads

Summary:

total	20.46 million mi
median	11 630 mi
highest	4.03 million mi (United States)
lowest	4.97 mi (Tuvalu)

(1994 to 2008)
(based on 225 values; 24 unavailable)

Total road length map:



(no data available)
0
4 to 360 000
360 000 to 720 000
720 000 to 1.1 million
1.1 million to 1.4 million
1.4 million to 1.8 million
1.8 million to 2.1 million
> 2.1 million
(in miles)

Default AV Validation: Public Road Testing

Carnegie Mellon University

- **Good for identifying "easy" cases**
  - Expensive and potentially *dangerous*
  - Should concentrate on **data collection**, not debugging

Did We Learn The Right Lesson from Tempe?

Carnegie Mellon University

- **NOT: Blame the victim**
  - Pedestrian in road is **expected**
- **NOT: Blame the technology**
  - Immature technology under test
    - **Failures are expected!**
- **NOT: Blame the driver**
  - A solo driver drop-out is **expected**

- **The real AV testing lesson:**

  ➔ Ensure safety driver is engaged ←

  - Safety argument: Driver alert; time to respond; disengagement works

Can Safety Driver React In Time?

Carnegie Mellon University

- **Safety Driver Tasks:**
  - Mental model of “normal” AV
  - Detect abnormal AV behavior
  - React & recover if needed

Jan 20, 2016; Handan, China

- **Example: obstructed lane**
  - Does driver know when to take over?
  - Can driver brake in time?
    - Or is sudden lane change necessary?

- **Example: two-way traffic**
  - What if AV commands sudden left turn into traffic?

Closed Course Testing

Carnegie Mellon University

- **Safer, but expensive**
  - Not scalable
  - Only tests things you have thought of!

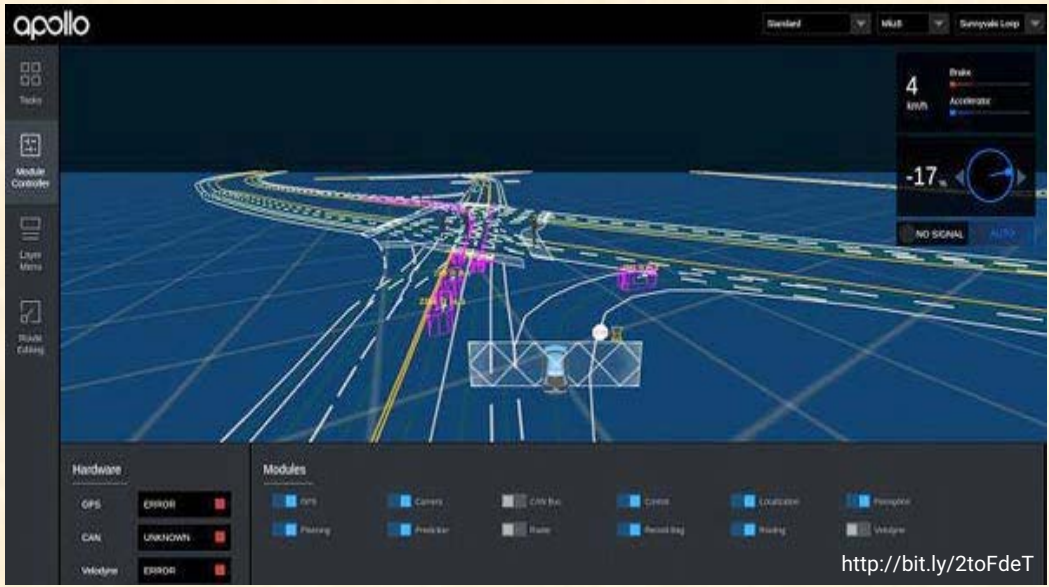
Volvo / Motor Trend

Simulation

Carnegie Mellon University

- **Highly scalable; less expensive**
  - Scalable; need to manage fidelity vs. cost
  - Only tests things you have thought of!

Udacity



Apollo

What About Edge Cases?

Carnegie Mellon University

- **You should expect the extreme, weird, unusual**
  - Unusual road obstacles
  - Extreme weather
  - Strange behaviors

PREDICTED CONCEPT	PROBABILITY
bird	0.997
no person	0.990
one	0.975
feather	0.970
nature	0.963
poultry	0.954
outdoors	0.936
color	0.910
animal	0.908

https://www.clarifai.com/demo

- **Edge Case are surprises**
  - You won't see these in testing

➔ Edge cases are the stuff you didn't think of!

Just A Few Edge Cases

Carnegie Mellon University

- Unusual road obstacles & obstacles
- Extreme weather
- Strange behaviors


http://bit.ly/2tvCCPK


http://bit.ly/2top1KD


https://dailym.ai/2K7kNS8


https://goo.gl/J3SSyu

https://en.wikipedia.org/wiki/Magic_Roundabout_(Swindon)

Why Edge Cases Matter

Carnegie Mellon University

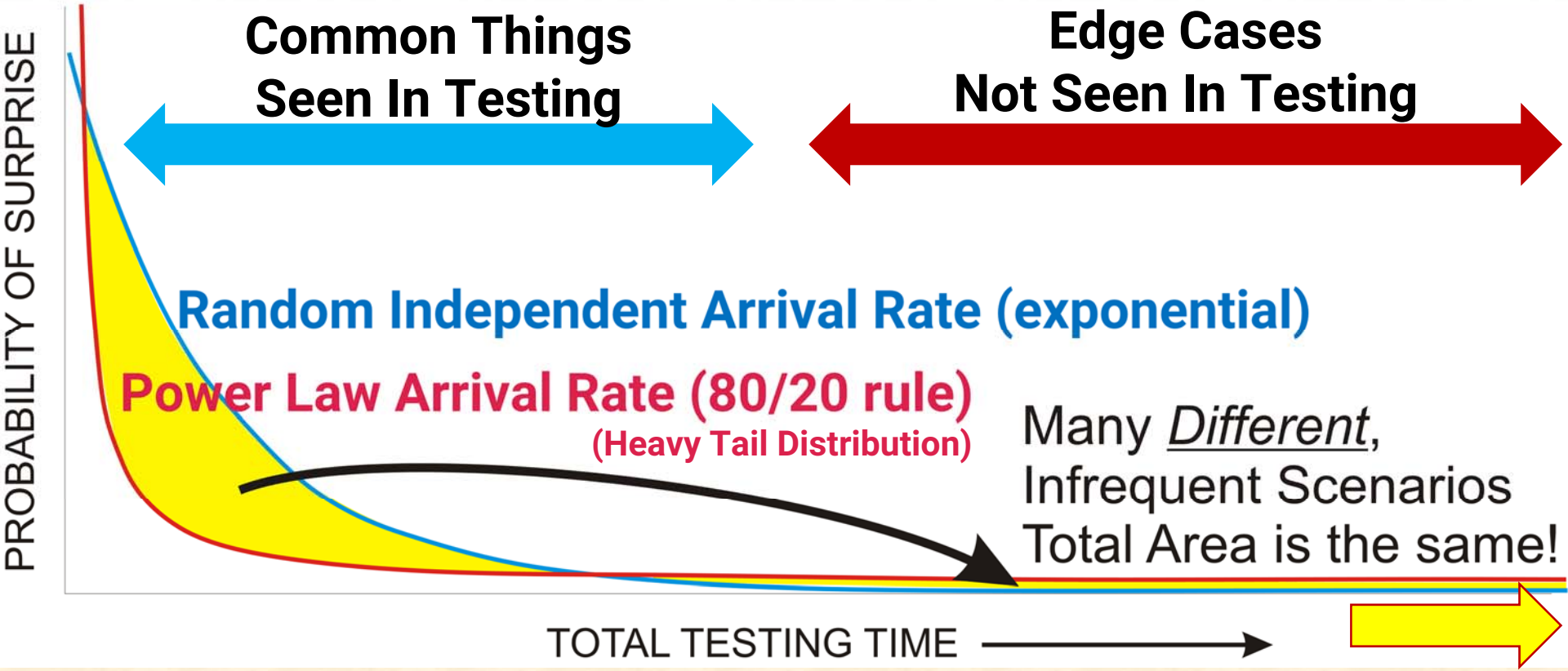
- **Where will you be after 1 Billion miles of validation testing?**

- **Assume 1 Million miles between unsafe "surprises"**
  - Example #1:
    100 "surprises" @ 100M miles / surprise
    - All surprises seen about 10 times during testing
    - With luck, all bugs are fixed
  - Example #2:
    100,000 "surprises" @ 100B miles / surprise
    - Only 1% of surprises seen during 1B mile testing
    - Bug fixes give no real improvement (1.01M miles / surprise)

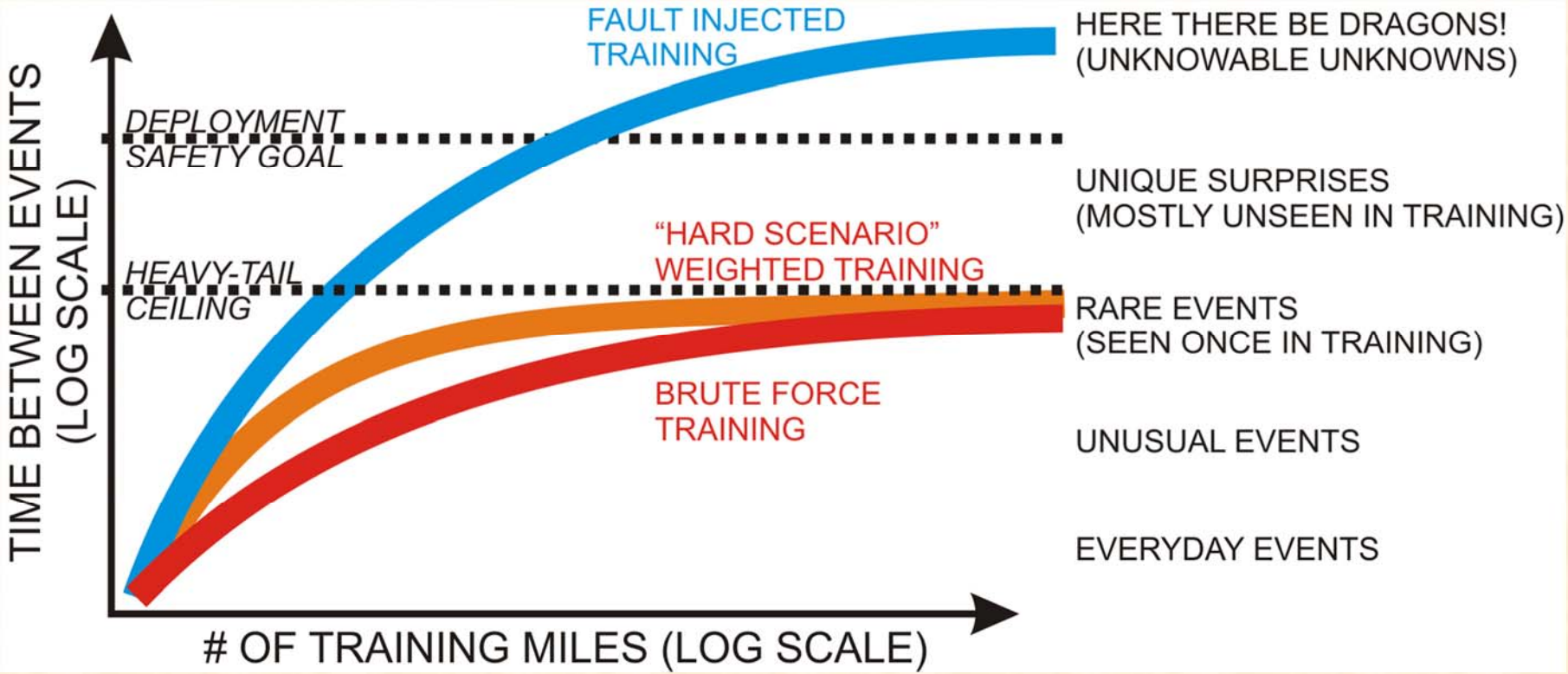
https://goo.gl/3dzguf

The Real World: Heavy Tail Distribution(?)

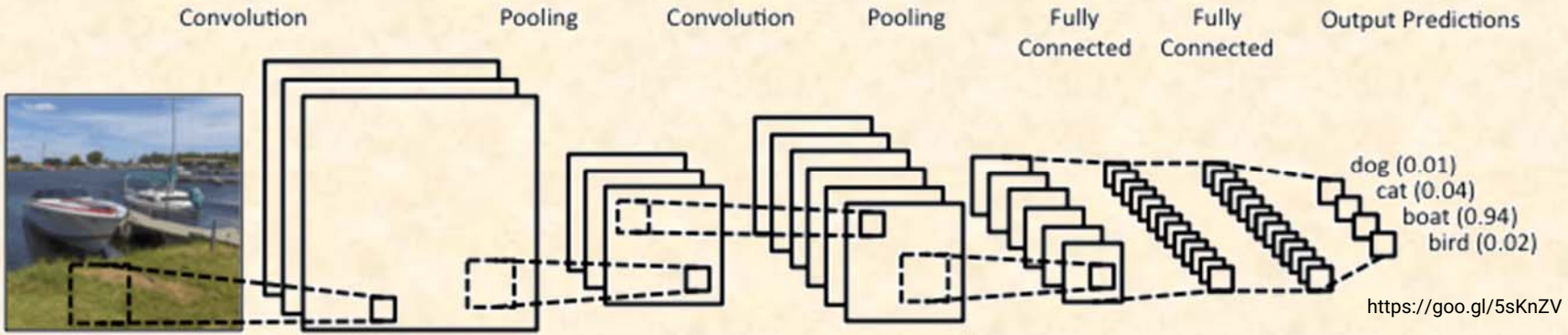
Carnegie Mellon University



The Heavy Tail Testing Ceiling



Malicious Image Attacks Reveal Brittleness

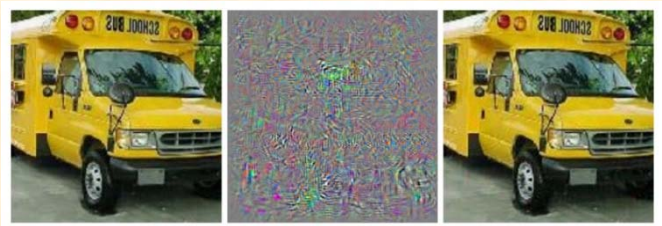


https://goo.gl/5sKnZV

QuocNet:

Car | **Not a Car** | ***Magnified Difference***

AlexNet:



Bus | ***Magnified Difference*** | **Not a Bus**

Szegedy, Christian, et al. "Intriguing properties of neural networks." *arXiv preprint arXiv:1312.6199* (2013).

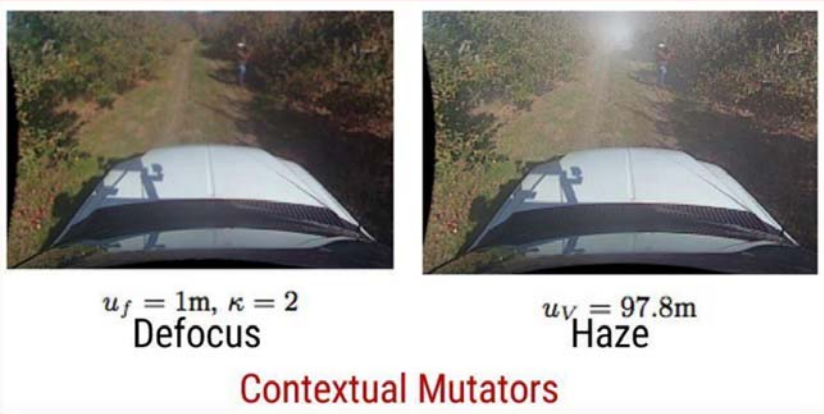
ML Is Brittle To Environment Changes

Carnegie Mellon University

- **Sensor data corruption experiments**

Synthetic Equipment Faults

Gaussian blur



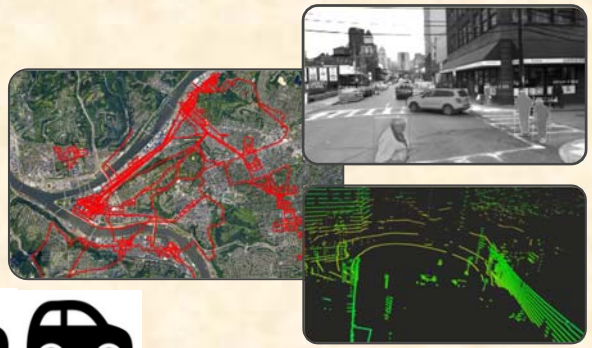
Defocus & haze are similarly a significant issue

Exploring the response of a DNN to environmental perturbations from “Robustness Testing for Perception Systems,” RIOT Project, NREC, DIST-A.

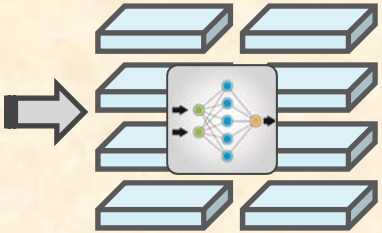
What We're Learning With Hologram

Edge Case Research

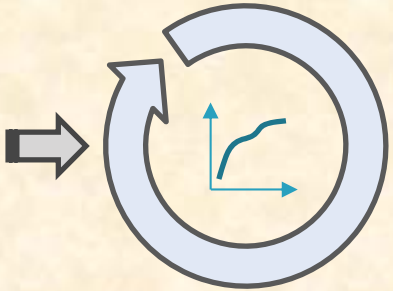
- **A scalable way to test & train on Edge Cases**



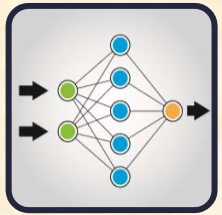
Your fleet and your data lake



Hologram cluster tests your CNN



Hologram cluster trains your CNN



Your CNN becomes more robust

hologram

SAFER PERCEPTION FOR AUTONOMY

Edge Case Testing: Data Fuzzing

- **Add small amounts of sensor noise**
- **Cost vs. speed tradeoff**
  - Use approximate models for training
  - Use realistic models for validation

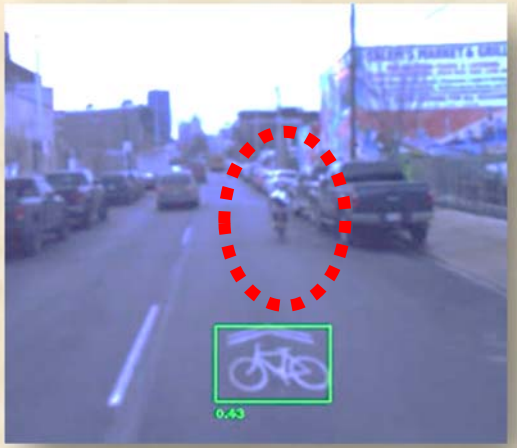
Pedestrian Missed: Gaussian Noise + Black Car

Pedestrian Missed: Gaussian Blur

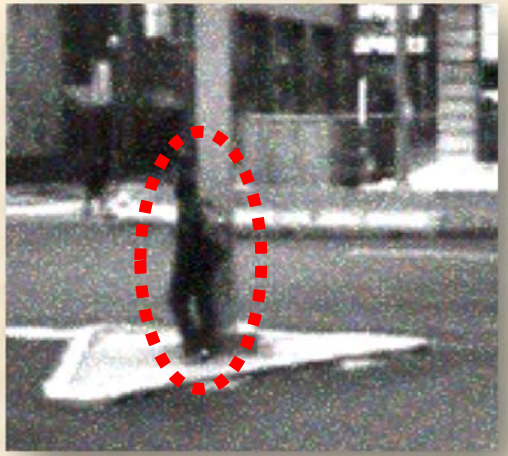
Context-Dependent Perception Failures

Edge Case Research

- **Perception failures are often context-dependent**
  - False positives and false negatives are both a problem



False positive on lane marking
False negative real bicyclist



False negative when
person next to light pole

False negative when
in front of dark vehicle

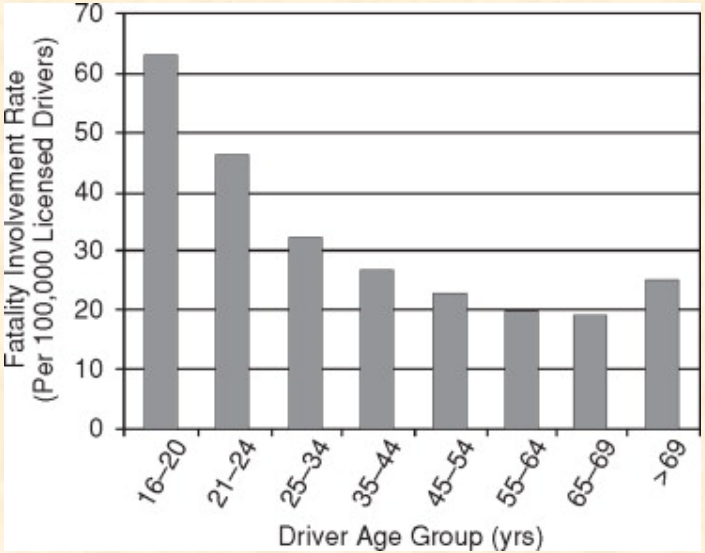
Will this pass a "vision test" for bicyclists?

Hard Question: How Safe Is Enough?

Carnegie Mellon University

- **~100M miles/fatal mishap for human driven road vehicles**
  - 28% Alcohol impaired
  - 27% Speeding-related
  - 28% Not wearing seat belts
  - 9% distracted driving (2016 data)
  - 2% drowsy
  - …

(total > 100% due to multiple factors in some mishaps)



https://goo.gl/tEuoaS

- **<u>Unimpaired</u> drivers are better than 100M miles**
  - What if AV fatality demographics change?
  - Currently 19% non-occupant fatalities (at-risk road users)

Hard Question: Does Delay Cost Lives?

Carnegie Mellon University

- **Is the "94% human error" meme accurate?**
  - DOT HS 812 115:
    - "The critical reason was assigned to drivers in an estimated 2,046,000 crashes that comprise 94 percent of the NMVCCS crashes at the national level.
    - However, in none of these cases was the assignment intended to blame the driver for causing the crash."
  - Low hanging fruit is **49%** for AVs (https://goo.gl/2WReTj)

NHTSA

Benefits of Automation

SAFETY

The safety benefits of automated vehicles are paramount. Automated vehicles' potential to save lives and reduce injuries is rooted in one critical and tragic fact: 94 percent of serious crashes are due to human error. Automated vehicles have the potential to remove human error from the crash equation, which will help protect drivers and passengers, as well as bicyclists and pedestrians. When you consider more than 35,092 people died in motor vehicle-related crashes in the U.S. in 2015, you begin to grasp the lifesaving benefits of driver assistance technologies.

https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety

- **RAND report suggests early deployment** (RR-1478-RC)
  - Even 10% better than a human driver saves lives overall
  - BUT –assumes no uncertainty on predicted AV fatality rate
    - Accounting for uncertainty raises the bar – probably a lot

Hard Question: How Do We Regulate?

Carnegie Mellon University

1. **Trust the car companies to self-regulate?**
   - Toyota criminal sanctions. VW Dieselgate. GM Ignition Switch. Takata air bags. … *see your news feed* …
   - Numerous safety critical software recalls
   - $XX++ billion invested with incentive to deploy ASAP
   - Litigation source code analysis of machine learning?
2. **Use existing automotive safety approaches?**
   - FMVSS requires standardized vehicle-level road tests
   - "Driver test" must include both skills & "maturity"
3. **Wait for a new safety standard?**
   - SOTIF (ISO PAS 21448) addresses partial autonomy for now
   - UL 4600 Autonomy Safety standard kick-off in August 2018

FMVSS 138 Telltale

Carnegie Mellon University

Thank You!

http://bit.ly/2MTbT8F (sign modified)

Edge Case Research