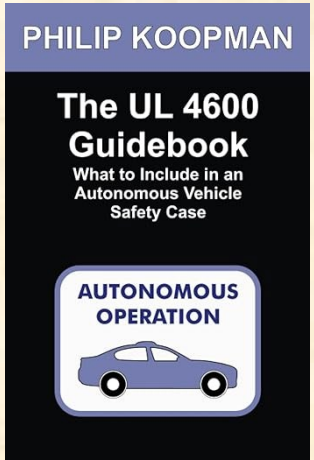
Challenges in Autonomous Vehicle Safety Assessment

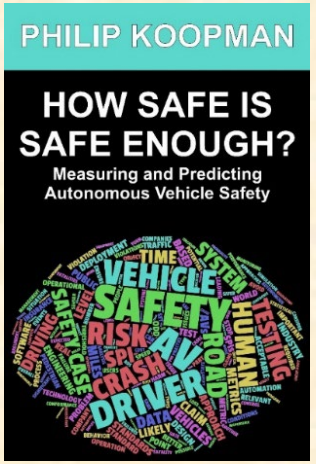
Prof. Philip Koopman

Carnegie Mellon University



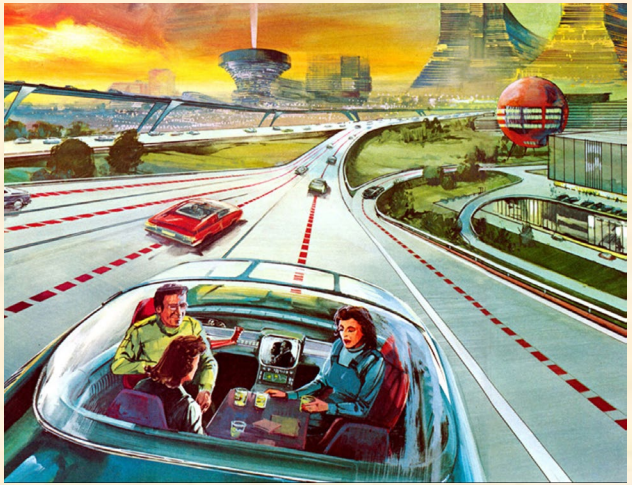
May 29, 2024

www.Koopman.us



Overview

- Six challenges in autonomous vehicle assessment:
  - Brute force testing is impracticable
  - Robot error
  - Machine learning & the Vee model
  - Industry standards adoption
  - Lifecycle & support infrastructure
  - Beyond statistical net safety



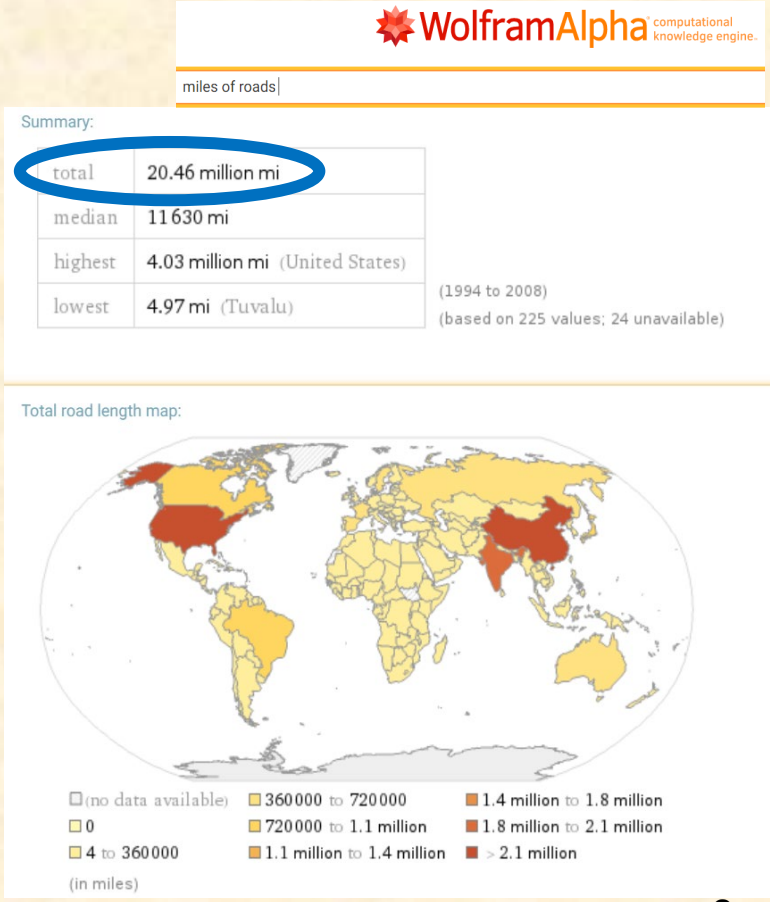
[General Motors]

Brute Force Road Testing

Carnegie Mellon University

- If 100M miles/fatality…
  - Test 3x–10x longer than mishap rate
    ➔ Need 1 Billion miles of testing
- That's ~50 times on every road in the world
  - With fewer than 10 fatalities
- Still need up to 100x more miles to know how fatalities turn out
  - Even more for heavy tail events

➔ Brute force testing impracticable



Robots Won't Make Human Driver Errors

Carnegie Mellon University

Humans are terrible drivers

42,795 Americans were killed in car crashes last year

You might be a good driver, but many of us aren't.
People cause millions of accidents every year in the US.
Cruise driverless cars are designed to save lives.
Our cars were involved in 92% fewer collisions as the primary contributor.* They also never drive distracted, drowsy or drunk.

Kyle Vogt
@kvogt

Follow

We ran this full-page ad in @nytimes and several local papers today.

Human drivers aren't good enough. America can do better, and it is time we fully embrace AVs.

Last edited 11:45 AM · Jul 13, 2023 · **956K** Views

July 2023

Human Error ➔ Robot Error

Carnegie Mellon University

March 2023 Crash into back of city bus

See also:
Aug. 2023 Injury crash with fire truck
Oct. 2023 Pedestrian dragging mishap

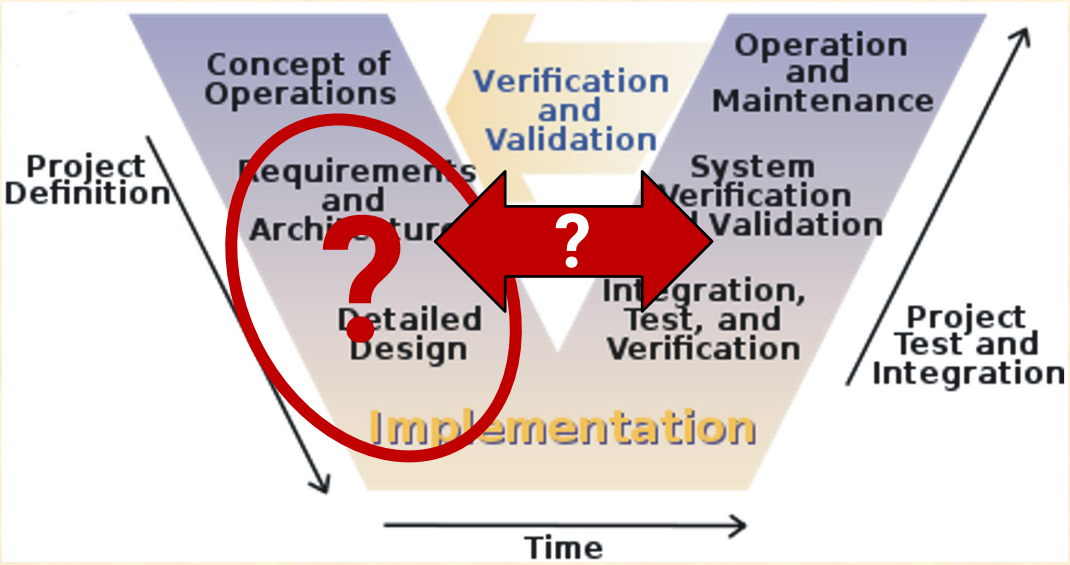
May 2024:
Crash into utility pole

See also: NHTSA PE24016-1

Machine Learning & Safety Process

Carnegie Mellon University

- Traditional safety engineering Vee model
  - Trace requirements to implementation
  - Testing validates the engineering process
  - Engineering rigor sets a prior expectation of safety



- Machine Learning (inductive training) breaks the Vee
  - More testing required due to degraded prior belief in safe design
  - Massive simulations still need to validate rare event coverage

Standards Set Expectation of Safety

Carnegie Mellon University

SYSTEM SAFETY	ANSI/UL 4600	*ISO TS 5083*	**Safety Beyond Dynamic Driving**
DYNAMIC DRIVING FUNCTION	ISO 21448	SaFAD/ISO TR 4804	**Environment & Edge Cases**
FUNCTIONAL SAFETY	ISO 26262		**Equipment Faults**
CYBER-SECURITY	SAE J3061	SAE 21434	**Computer Security**
VEHICLE SAFETY	FMVSS	NCAP	**Basic Vehicle Functions**

REQUIRED

HIGHLY AUTOMATED VEHICLE SAFETY CASE

ANSI/UL 4600

ROAD TESTING SAFETY

SAE J3018

Operational & Life Cycle Safety

Carnegie Mellon University

- Drivers do more than just drive
  - Occupant behavior, passenger safety
  - Detecting and managing equipment faults
- Operational limitations & situations
  - System exits Operational Design Domain
  - Post-crash situation response
- Lifecycle management
  - Security (internet-facing and infrastructure hacks)
  - Sensor calibration & maintenance
  - How safety critical are cloud & remote support services?

Beyond Net Statistical Safety

Carnegie Mellon University

1. Safe as a human driver on average
   - Perhaps 100M miles/fatal crash (even better for good drivers)
2. Avoiding risk transfer onto vulnerable populations
   - Pedestrian harm should not increase even if net harm is reduced
3. Avoid negligent computer driving
   - Hold computers to human driver duty of care
4. Conform to industry safety standards
   - Uncrewed operation = deployment
5. Address other ethical & equity concerns
   - Limited local authority; manufacturer accountability for harm

Summary of AV Assessment Challenges

Carnegie Mellon University

1. Brute force testing won't validate mitigation of rare hazards
2. Human errors ➔ robot errors
3. Machine learning breaks traceability for the Vee model
4. Industry standards under-used
5. More consideration of lifecycle and external-to-vehicle support
6. "Safe" is more than just net statistical safety

More video presentations here:

https://bit.ly/KoopmanTalks

Resources

Carnegie Mellon University

- Video lecture series on autonomous vehicle safety:
  - Keynote talks: https://users.ece.cmu.edu/~koopman/lectures/index.html#talks
  - Mini-course: https://users.ece.cmu.edu/~koopman/lectures/index.html#av
- "Safe Enough" book & talk video:
  - https://safeautonomy.blogspot.com/2022/09/book-how-safe-is-safe-enough-measuring.html
- UL 4600 AV safety standard book & talk video:
  - https://safeautonomy.blogspot.com/2022/11/blog-post.html
- Liability-based proposal for state AV regulation & podcast
  - https://safeautonomy.blogspot.com/2023/05/a-liability-approach-for-automated.html
- US Congressional House E&C testimony:
  - https://safeautonomy.blogspot.com/2023/07/av-safety-claims-and-more-on-my.html