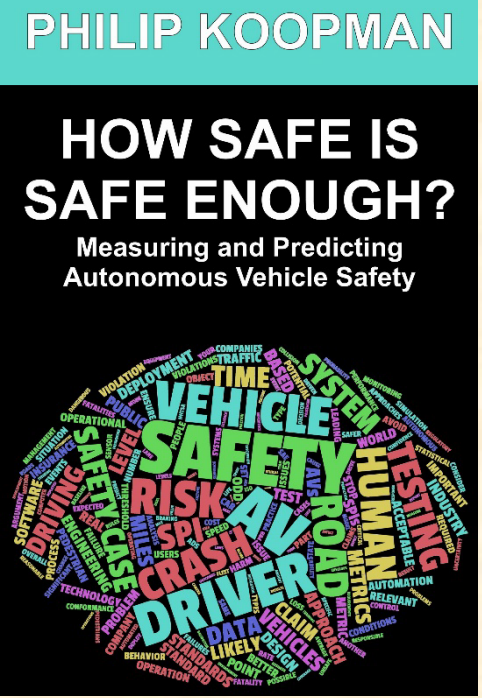
PHILIP KOOPMAN



Regulatory Policy for Autonomous Vehicle Safety & Deployment

Prof. Philip Koopman

November 2022

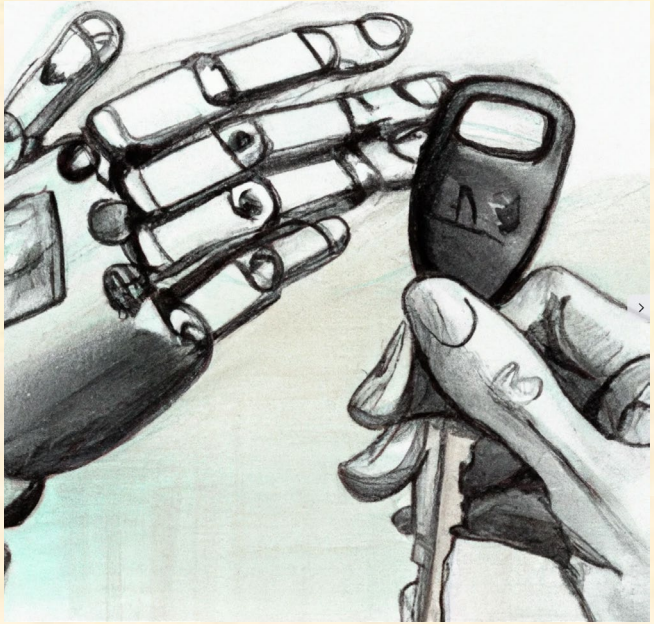
www.Koopman.us

Carnegie Mellon University

Overview

Carnegie Mellon University

- Autonomous Vehicles (AVs):
  - Sold on safety
  - But so far safety is aspirational
- Industry response to slow progress
  - Automotive safety disinformation
  - Promoting a non-safety standard for regulators to use (SAE J3016)



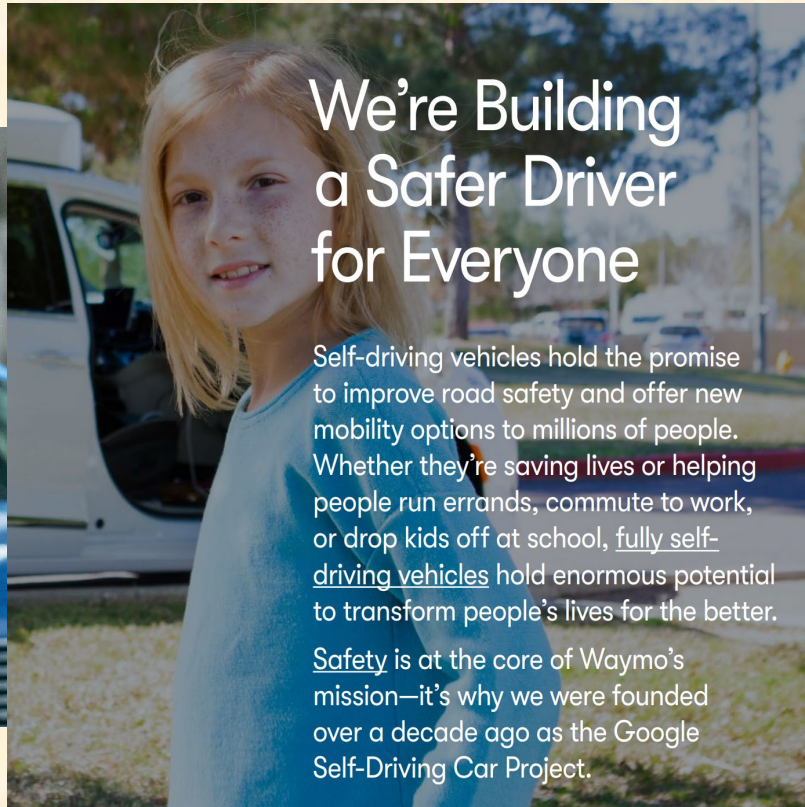
[Dall-e]

- This can be fixed
  - Base regulations on human driver safety responsibility
  - Involve more stakeholders on deployment decisions

ADS Technology: Sold Based on Safety

Ford VSSA https://bit.ly/3njionT

Waymo VSSA https://bit.ly/2QuYhai



How's It Going With Autonomy Testing?

Carnegie Mellon University

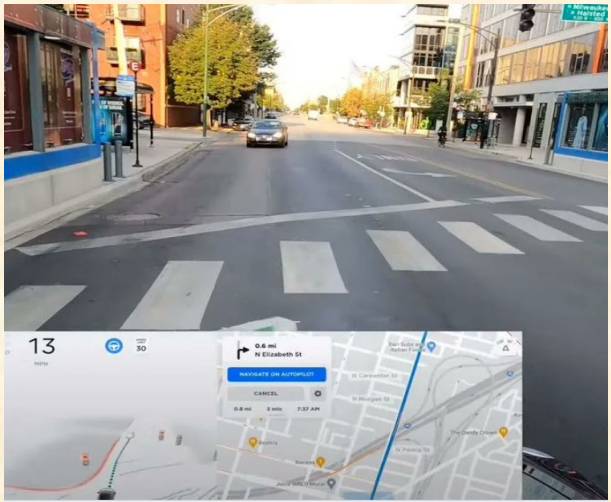
- Uber ATG fatality, Tempe AZ/US: March 2018
  - Uber ATG closed: January 2021
- Easymile phantom braking injuries: 2019, 2020
- Pony.AI crash: CA/US: Oct. 2021
  - Uncrewed test permit revoked
- WeRide sleeping tester: Oct. 2021
- Local Motors injury, Whitby CA: Dec. 2021
  - Company closed: Jan. 2022
- TuSimple truck testing crash: April 2022
  - Alert, trained safety driver unable to prevent crash
- Cruise left turn injury: June 2022

https://bit.ly/3AupcWb

How's It Going With Tesla?

Carnegie Mellon University

- Tesla FSD "beta test" US: multiple incidents
  - Videos of reckless driving by testers
  - Exploiting Level 2 loophole for L3/L4 testing
- Tesla AutoPilot: injuries and fatalities
  - Multiple crashes investigated by NTSB
    - Common theme: inadequate driver monitoring
  - NHTSA engineering analysis
    - 16 crashes; 15 injuries; 1 fatality
      for crashes into emergency vehicles/workers



https://bit.ly/33L0Bk7 https://bit.ly/3nQUfXl

  - NHTSA mandated reporting from all Level 2 and higher vehicles
  - Felony charges for fatal AP-related crash (Jan. 2022) https://bit.ly/3tFlQOU

Why Is AV Safety Complicated?

Carnegie Mellon University

- Public expectations
  - Expect super-human machine performance
  - Trust too easily given, backlash when broken
- Technical challenges
  - Machine Learning safety is work in progress
  - Statistical techniques struggle with rare events
- Historical industry culture clash
  - Autonomy researchers: it's all about the cool small-scale demo
  - Silicon Valley: move fast + break things
  - Automotive: blame driver for not mitigating equipment failures
  - Regulators: test-centric; weak digital safety expertise

What People Mean By "Safe"

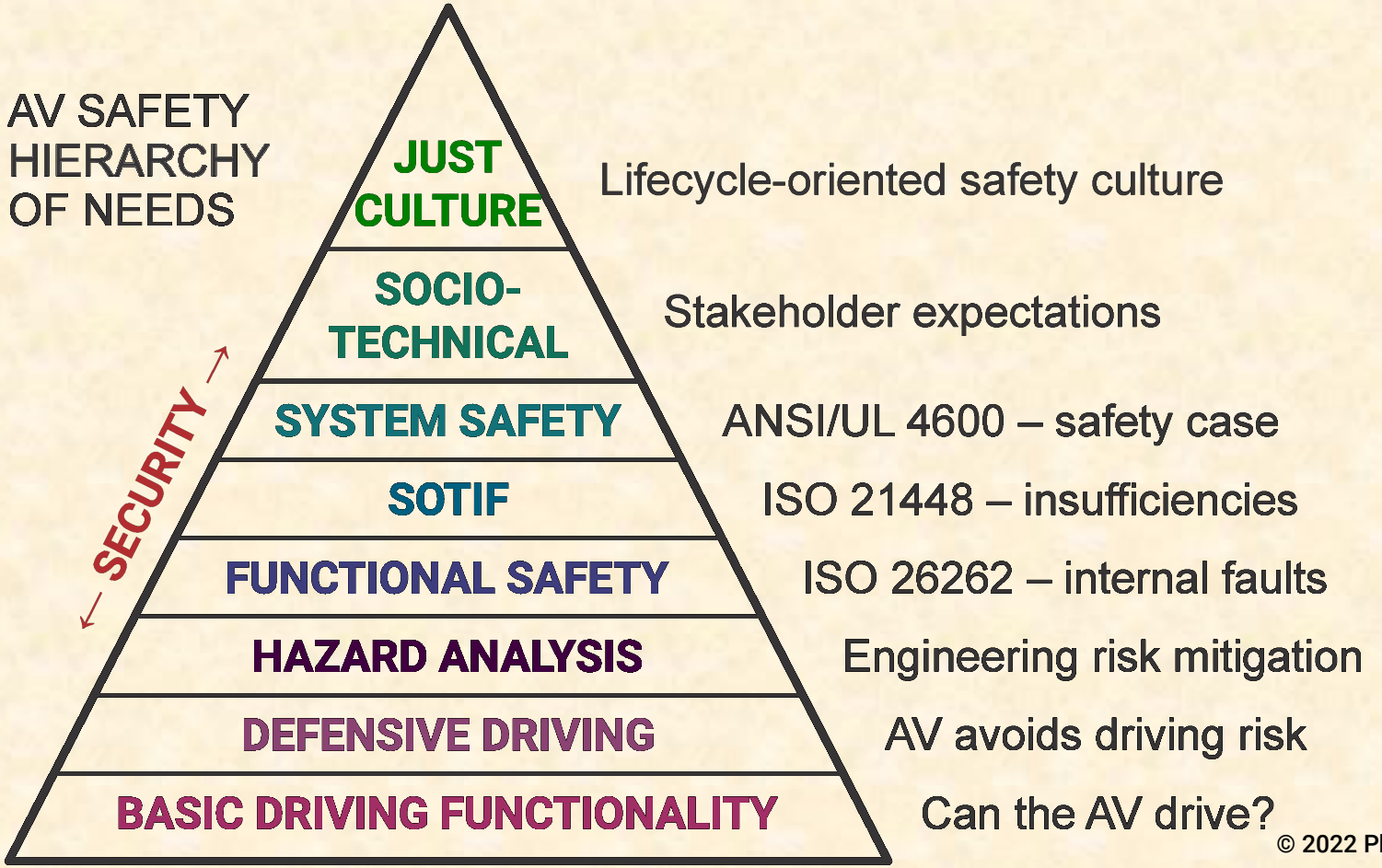
Carnegie Mellon University

- Human drivers are bad, so computers will be safe
  - Industry rhetorical talking points are ubiquitous
- "Safety is our #1 priority"
- Safe driving behavior
  - Follows traffic laws; good roadmanship
- Tested/simulated for millions of miles
- Risk is managed via insurance
- Conforms to safety standards
- Positive Risk Balance (better than human)
- Safety cases supported by evidence

[Dall-e]

Hierarchy Of Concurrent Safety Needs

Carnegie Mellon University



Standards-Based Engineering Approach

Carnegie Mellon University

SYSTEM SAFETY	ANSI/UL 4600		**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**

HIGHLY AUTOMATED VEHICLE SAFETY CASE

ANSI/UL 4600

ROAD TESTING SAFETY

SAE J3018

US Regulatory Posture As Of Early 2022

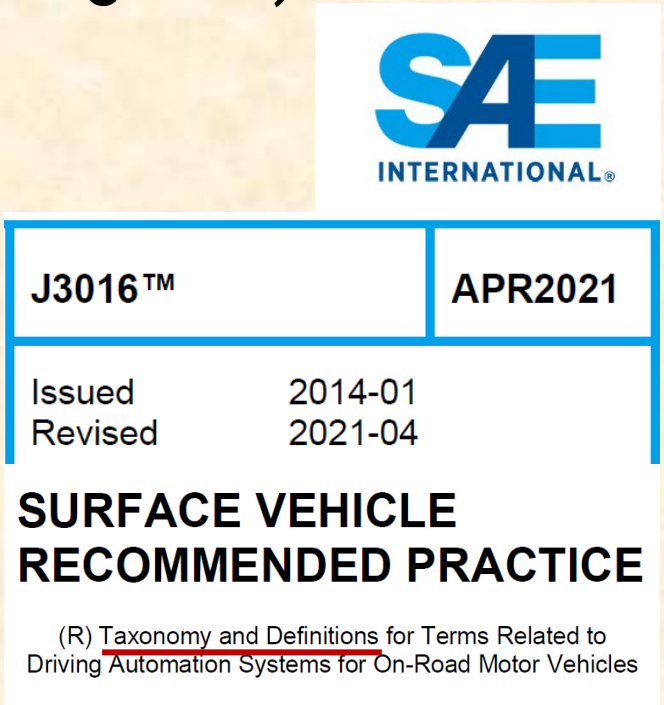
Carnegie Mellon University

- **Federal / equipment safety: almost nothing for AVs**
  - NHTSA ANPRM proposing industry standards Dec. 2020
  - Started collecting crash data in 2021
- **State / driver safety: administrative only**
  - California: permits, driver checks, reporting
  - Texas, Arizona, etc. “open for business”
  - Aggressive state-by-state lobbying
- **Municipal / local conditions: mixed**
  - NYC DOT requires SAE J3018 for testing
  - Munis hobbled by state preemption

#1 Issue: Deployment Governance

Carnegie Mellon University

- Who decides it's time to deploy, based on what?
- US: self-certification to FMVSS (no homologation)
  - Vehicle test of some basic functions only
  - No requirement for engineering standards
  - State permits are licensing & insurance
  - Regulations based on SAE J3016 Level
    - *J3016 is not a safety standard!*
- Companies decide when to test/deploy
  - Opaque about their safety goal
  - Opaque about criteria to deploy
  - Enormous pressure: $Billion milestones



Industry Non-Commitment To Standards

Carnegie Mellon University

- **Waymo Safety Methodologies report, Oct 2020**
  - What it might seem to say: Look at us, ISO 26262! Woohoo!
  - But only looked at HARA (portion of part 3), not whole standard
  - "does not rely" – doesn't say they use HARA at all!
  - "not a perfect fit" – even though tailoring to fit is routine
  - Bottom line: "We don't want to follow the industry standard."

action to address the hazard. ISO 26262 has provided significant insights for Waymo's hazard analysis processes. However, Waymo does not rely strictly or exclusively on ISO 26262's principles, which are not a perfect fit for a Level 4 ADS, where there is a need for a special focus on the plethora of conditions likely to be encountered in the intended ODD, and where separate analysis of individual items may not be as useful as analysis of hazards related to system interactions.

https://bit.ly/3Kf3lGJ

Industry Disinformation

Carnegie Mellon University

- "94% fatalities due to human error"
  - No data showing AVs are safer than human drivers
- "Regulate or Innovate"
  - Safety standards are technology neutral
- "Existing checks and balances sufficient"
  - Software safety largely unaddressed
- "Safety standards don't apply to us"
- "A million miles of testing ➔ safe"
- "Disclosing safety outcomes reveals our secret sauce"
- …


DESIGNLINES | AUTOMOTIVE DESIGNLINE

Autonomous Vehicle Myths: The Dirty Dozen

By Philip Koopman, Carnegie Mellon University

10.22.2021 2

https://bit.ly/3AqDGq1

Industry Behaviors That Erode Trust

Carnegie Mellon University

- Messaging the Dirty Dozen Myths
  - Safety theater of various forms
- Enabling insufficiently safe deployment
  - Possibly employing Moral Crumple Zones
- Lobbying states for favorable terms
  - Preempt municipal ordinances
  - FOMO-driven narrative (other states; China)
  - Computer is "driver" – no person to hold accountable
  - Low insurance limits vs. $12M statistical life
  - No defined level of safety; little government oversight over safety
  - Selected bills here: bit.ly/3O5ZfDg (Feb 10, 2022 blog post)


Spring 2022 www.uclajolt.com Vol. 27, No. 3

UCLA

JOURNAL OF LAW & TECHNOLOGY

AUTONOMOUS VEHICLE REGULATION & TRUST: THE IMPACT OF FAILURES TO COMPLY WITH STANDARDS

William H. Widen* & Philip Koopman**

https://bit.ly/3rMKKKh

Insurance Costs Won't Force Safety

Carnegie Mellon University

- Cost of excessive risk drives improvement
  - Reducing risk tends to improve safety, but…
- Affordable risk might exceed acceptably safe
  - Life insurance for combat military personnel
  - Commercial space launch insurance
  - Motorcycle insurance
  - Cost of fatality settlement compared to $2M-$5M/day burn rate
- Risk management is not enough for acceptable safety
  - Risk transfer (occupants vs. pedestrians)
  - Existential pressure for company to deploy with unproven safety

Need A Better Regulatory Approach

Carnegie Mellon University

- SAE J3016 is unsuitable for regulations
  - Explicitly not a safety standard
  - Easily gameable to degrade public safety
  - Level definitions have safety gaps
    - e.g., driver monitoring is optional

[SAE]

- Should regulate safety outcomes, not how vehicles are built
- Need a clear assignment of driver safety role
  - Make sure the driver (if any) can ensure safety
  - Emphasize driver attention & ability to intervene when needed

Driver Assistance Features

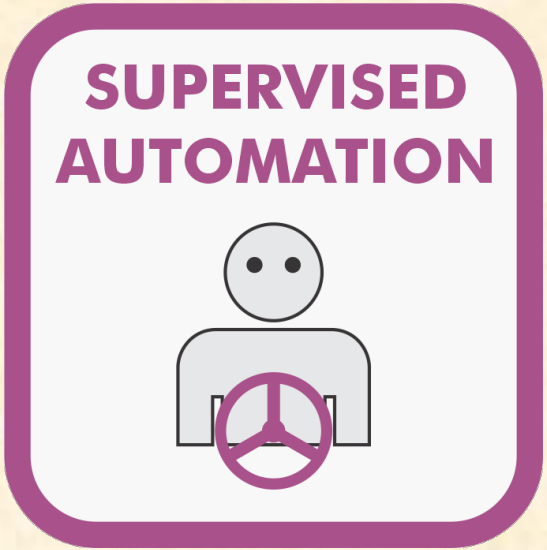
Carnegie Mellon University

- Driver is required to steer
  - Roadway departure without driver steering
  - Hands on steering wheel continuously
- Conventional driving
  - Speed-based cruise control OK
  - Distance-based cruise control OK
  - Momentary collision avoidance OK
  - But NOT automated continuous steering
- Regulation:
  - Conventional vehicle rules

Driver Supervises Automation

Carnegie Mellon University

- Driver supervises automation
  - Effective driver monitoring required
  - Might permit some hands off steering wheel
- Speed + steering "cruise control"
  - Lane and speed maintenance
  - Driver initiated lane changes OK
  - System warns whenever takeover required
  - Automated intersection turns *excluded*
- Regulation:
  - Evidence of effective driver monitoring



Vehicle Testing

Carnegie Mellon University

- Driver intervenes to mitigate design defects
  - Testing ➔ presumption that system has defects
- Public road testing is hazardous to road users
  - Use only trained, vetted testers
  - Driver + vehicle pair shown to be acceptably safe
  - Do not test known defective behaviors
- Regulation:
  - Testing permits & report safety incidents
  - Conform to SAE J3018 public road testing for driver management
  - Require Safety Management System (SMS)

Autonomous Operation

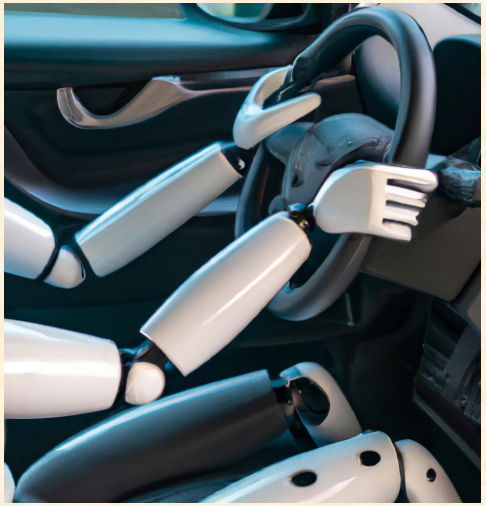
Carnegie Mellon University

- Driver can fall asleep (safely)
  - Driver is entirely optional
- True autonomous vehicle
  - AV handles driving safety
  - AV handles other aspects of safety
  - Both passenger & cargo vehicles
- Regulation:
  - Conform to industry safety standards:
    ISO 26262, ISO 21448, ANSI/UL 4600, security standards

Elements of Safe Enough AV Deployment

Carnegie Mellon University

- Deployment Governance
  - Stakeholders involved in criteria & decision
  - Safety culture assures fair dealing on decision
- Acceptable risk
  - Good human PRB + safety factor for unknowns
  - Safety & security industry engineering standards
  - Ethical concerns addressed
- Safety case
  - Transparent argument based on evidence
  - Lifecycle uncertainty management via field feedback
- Safety while public road testing



[Dall-e]

Summary

Carnegie Mellon University

- AV industry at a crossroads:
  1. Adversarial to regulation; risk of backlash, or
  2. Collaborative governance to establish trust or
  3. Lean into the Level 2++ unregulated loophole

- Should companies own safety governance?
  - Huge financial benefits for early to market
  - $ Billion funding and milestone pressure
  - Tesla behavior: no consequences; stock value increases
    - Will other companies successfully resist cutting safety corners?
- Detailed paper on AV Regulation and Trust:
  - http://dx.doi.org/10.2139/ssrn.3969214 (UCLA J. Law & Tech.)