Prof. Philip Koopman

Carnegie Mellon University

Trust & Governance for Autonomous Vehicle Deployment

January 2022

@PhilKoopman

Overview

Carnegie Mellon University

- AV safety is complicated
  - Mishaps and other issues
  - US regulatory landscape
- Dirty Dozen AV industry myths
- Deployment governance
  - Governance is #1 AV ethics issue now
- For 2022, the big issues are regulation & trust

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

How's It Going With Autonomy Testing?

Carnegie Mellon University

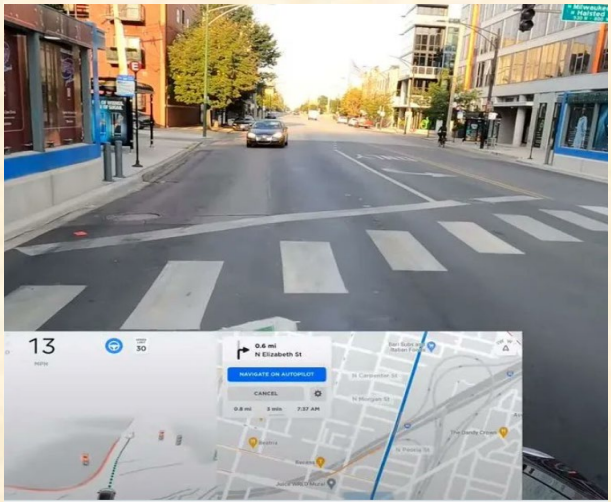
- Uber ATG fatality, Tempe AZ/US: March 2018
  - Uber ATG closed: January 2021
- Local Motors injury, Whitby CA: Dec. 2021
  - Company closed: Jan. 2022
- Pony.AI crash: CA/US: Oct. 2021
  - Uncrewed test permit revoked
- WeRide sleeping tester: Oct. 2021
  - Company deflects issue / no apparent regulator action
- Easymile shuttle phantom braking injuries: (2019, 2020)
- Cruise battling with SF MTA over passenger pickup: Dec 2021

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 investigations
    - 11 crashes; 17 injuries; 1 fatality
      for crashes into emergency vehicles/workers
  - NHTSA mandating reporting from all Level 2 and higher vehicles
  - Felony charges for fatal AP-related crash (Jan. 2022) https://bit.ly/3tFlQOU



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

US Regulatory Posture As Of Early 2022

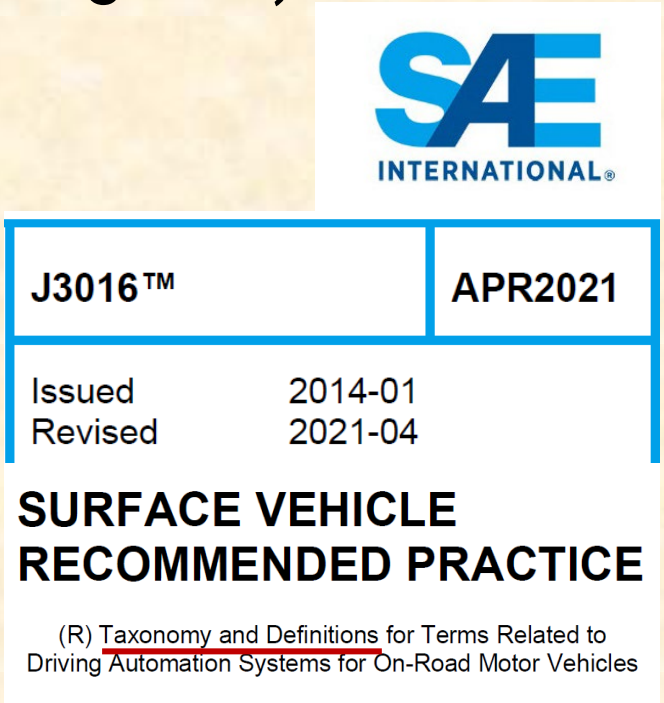
Carnegie Mellon University

- **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
  - Industry pushing for state preemption in Pennsylvania

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 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



Eroding Trust: AV Regulatory Dirty Dozen Myths

Carnegie Mellon University

1) 94% fatalities due to human error

- Humans failed to prevent ≠ human caused

"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. [DOT HS 812 115]

However, in none of these cases was the assignment intended to blame the driver for causing the crash."

2) Innovate or regulate; choose only one

- False dilemma, especially for testing safety
- "Innovative" is not necessarily safe

3) Already sufficient regulations in place

- State DOTs require license+insurance, not testing safety

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

AV Regulatory Dirty Dozen Myths – 2

Carnegie Mellon University

4) Cars meet all existing safety regulations

- FMVSS is about basic features, not software safety
- FMVSS needs updates, but not main issue

5) Safety standards aren't applicable because {reasons}

- Example: adopting safety standards will force AVs to be less safe
- Road testing: SAE J3018 + SMS practices
  - Be mindful of lessons learned by Uber ATG
- Production: ANSI/UL 4600, incorporating ISO 26262, ISO 21448
  - This is what is in NHTSA ANPRM from Dec. 2020

Waymo Standard Statement

Carnegie Mellon University

- **Waymo Safety Methodologies report, Oct 2020**
  - 26262 is great stuff!
  - But only looked at HARA (part 3), not whole standard
  - "does not rely" – doesn't say they use HARA at all!
  - "not a perfect fit" *– Myth #5*
  - Summary: "We looked at ISO 26262 HARA, but decided not to."

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

AV Regulatory Dirty Dozen Myths – 3

Carnegie Mellon University

6) Avoid "patchwork" of state regulations

- Patchwork primarily of AV industry making

7) "Spirit of" / "incorporates ideas from" language regarding standards

- If it doesn't conform, it's just hand-waving
- Maybe they're doing the right thing …
  … but maybe not
- If you can't show it is safe,
  it should be presumed unsafe

https://bit.ly/35jdWAz

Aurora VSSA Standard Statement

Carnegie Mellon University

- **Aurora Voluntary Safety Self-Assessment 2021**
  - **"We leverage industry best practices and standards … relevant principles"** ***– Myth #7***
  - **Laundry list of standards "are applicable" … but no commitment to use them.**

> safety within Aurora. We leverage industry best practices and standards that have significantly raised the bar in automotive safety, and we are committed to ensuring the relevant principles are embedded within our internal policies, procedures, and approaches in developing the Aurora Driver.

> The U.S. DOT Comprehensive Plan[12] identified a set of twenty automotive best practices and standards, which individually address different components or processes for a self-driving system or enterprise. Further, standards such as SAE J3016, SAE J3018, UL 4600, International Organization for Standardization (ISO) 26262, and ISO 21448, as well as the best practices from the Automated Vehicle Safety Consortium (AVSC), are applicable to self-driving technology.

https://bit.ly/3IaajLw

AV Regulatory Dirty Dozen Myths – 4

Carnegie Mellon University

8) Government regulators aren't smart enough
- US DOT proposed using industry's own standards

9) Disclosing data gives away secret sauce
- How is # of reckless driving incidents secret autonomy sauce?

10) Delaying AV deployment is basically killing people
- No data exists showing AVs are actually safer in practice

11) We haven't killed anyone (yet), so we're safe
- At 100M miles+ per fatality, insufficient data to prove safety

12) Other cities/states don't regulate
- Intimidation, FOMO for economic benefits, "hostile to innovation"

Stakeholder Trust

Carnegie Mellon University

- Would you trust your life to an automated vehicle?

Industry Behaviors That Erode Trust

Carnegie Mellon University

- Messaging the Dirty Dozen Myths
  - Safety theater of various forms
- Maintaining option less safe deployment
  - Possibly employing Moral Crumple Zones
  - AV Secret Sauce excuse for opacity
- Lobbying states for favorable terms
  - Preempt municipal ordinances
  - FOMO-driven narrative (China; other states)
  - Sue the ADS; Low insurance limits ($1M vs. $11M statistical life)
  - No defined level of safety, nor gov't oversight over safety
  - Example: PA SB 965 (Jan 5, 2022) https://bit.ly/3Ic6LIE


DESIGNLINES | AUTOMOTIVE DESIGNLINE

Autonomous Vehicle Myths: The Dirty Dozen

By Philip Koopman, Carnegie Mellon University

10.22.2021 2

https://bit.ly/3AqDGq1

Restoring AV Industry Trust

Carnegie Mellon University

- Safety transparency
  - Road testing safety metrics
  - Deployment safety criteria
- Commit to industry standards
  - SAE J3018+SMS road testing safety
  - ISO 26262 + ISO 21448 + ANSI/UL 4600 for deployment safety
- Collaborate with regulators
  - Perhaps one high profile crash away from forcing regulators to act
  - Balance benefit to industry with protection for road users
  - Include all stakeholders to find win-win arrangement

SYSTEM SAFETY	UL 4600		Safety Beyond Dynamic Driving
DYNAMIC DRIVING FUNCTION	ISO/PAS 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

UL 4600

Summary

Carnegie Mellon University

- AV industry at a crossroads:
  1. Adversarial to regulation; risk of backlash, or
  2. Collaborative governance to establish trust

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