Prof. Philip Koopman

Driver Assistance vs. Automated Vehicle Safety

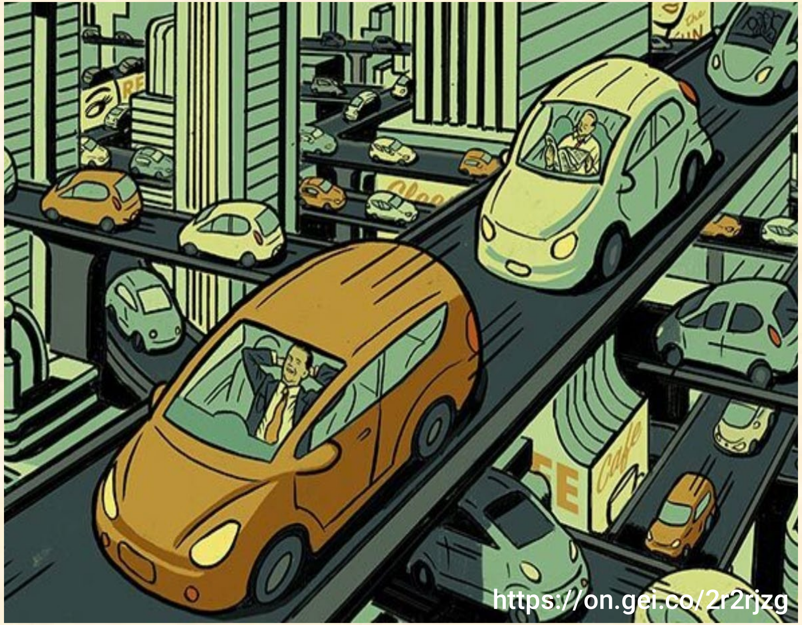
August 2021

Carnegie Mellon University

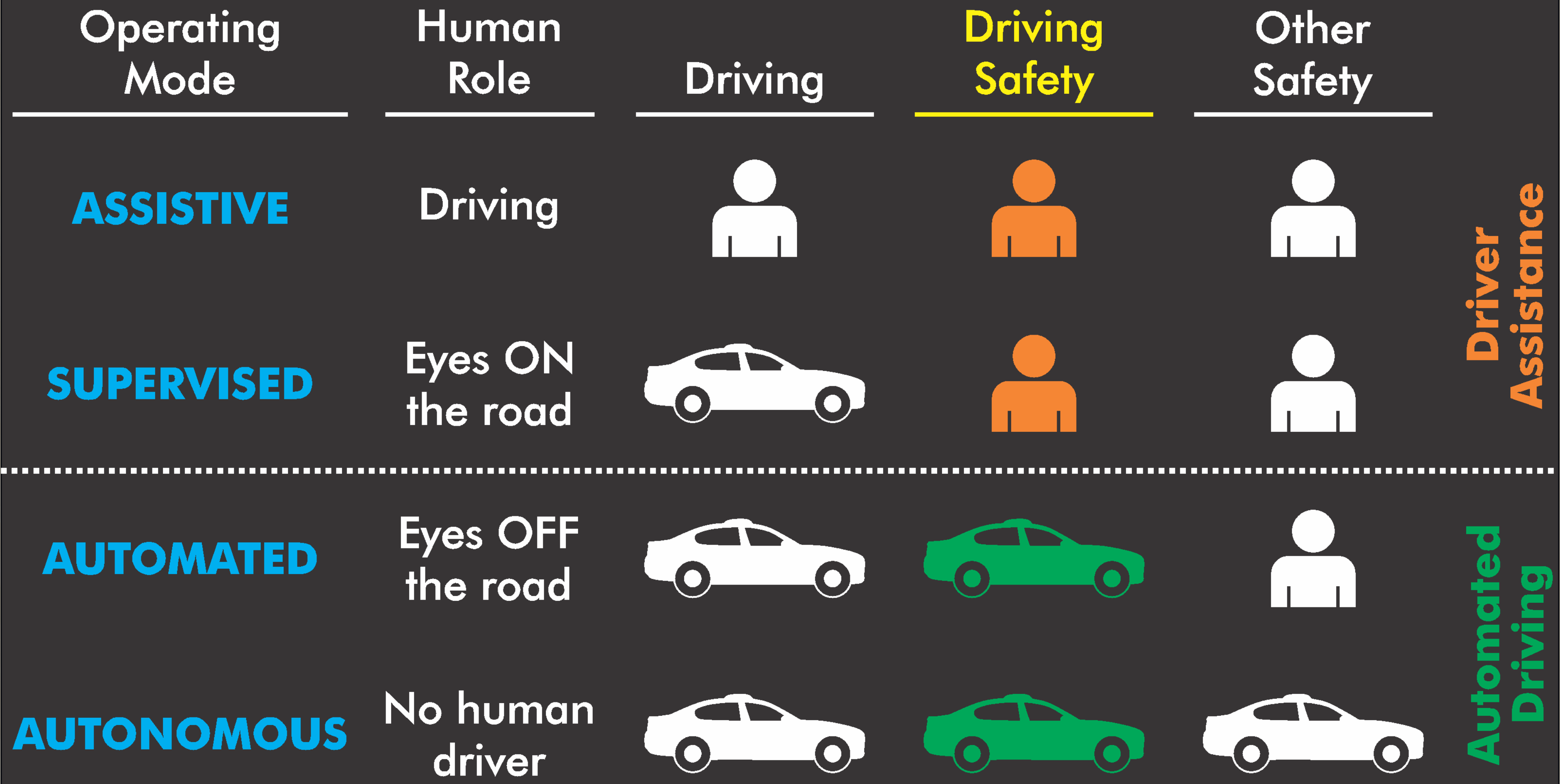
@PhilKoopman

Overview

- Driver Assistance:
  - Help human drivers be better & safer
- Driver Automation:
  - Vehicle actually drives
- Compare & contrast
  - Safety argument implications
  - Technology challenges
- Start with:
  - Automation modes for non-engineers



https://on.gei.co/2r2rjzg



Operating Mode	Human Role	Driving	Driving Safety	Other Safety	
ASSISTIVE	Driving	👤	👤	👤	Driver Assistance
SUPERVISED	Eyes ON the road	🚗	👤	👤	
AUTOMATED	Eyes OFF the road	🚗	🚗	👤	Automated Driving
AUTONOMOUS	No human driver	🚗	🚗	🚗	

Vehicle Automation Modes

Assistive: Help the Driver Drive

- Better execute driver commands
  - Anti-lock brakes
  - Electronic stability control
- Momentarily intervene for safety
  - Automated emergency braking
- The driver is responsible for safety
  - The vehicle obeys driver intent
  - Interventions to improve driver performance
  - Functional safety covers equipment failures (ISO 26262)

Shutterstock/Iliya

Supervised: Driver Monitors for Safety

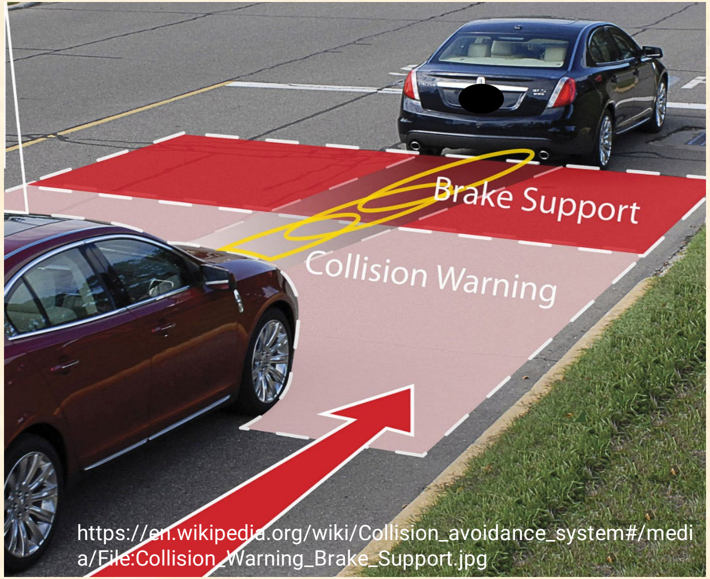
- Vehicle (mostly) does the driving
  - Speed control & lane keeping
- Human driver responsible for safety
  - Intervene to handle edge cases

Shutterstock/Metamorworks

- Driver monitors and intervenes
  - Vehicle must let driver intervene when needed (ISO 26262)
  - Effective driver monitoring required for automation complacency
  - Safety Of The Intended Function (SOTIF) (ISO 21448) helpful

ADAS Safety – Helping the Driver

- Proper functionality helps driver
  - Reduce driver stress, control mistakes
- Active safety can help
  - Helps avoid crashes
  - Tune to avoid false activations
- Arguably, good enough active safety
  - ADAS claims credit for safety; human blamed for crashes
  - BUT: avoid unreasonable demands on human drivers
    - – Unaided humans are terrible at monitoring boring automation



https://en.wikipedia.org/wiki/Collision_avoidance_system#/media/File:Collision_Warning_Brake_Support.jpg

Automated: The Car Drives

- Vehicle drives & handles safety
  - Driver need not pay attention to driving
  - Driving problems *not* dumped onto driver

Shutterstock/ Metamorworks

- The vehicle responsible for driving safety
  - By definition:
    collisions are not fault of a human driver

- Tension between safety and permissiveness
  - False non-detections (false negatives) generally hurt safety
  - False detections (false positives) generally hurt permissiveness

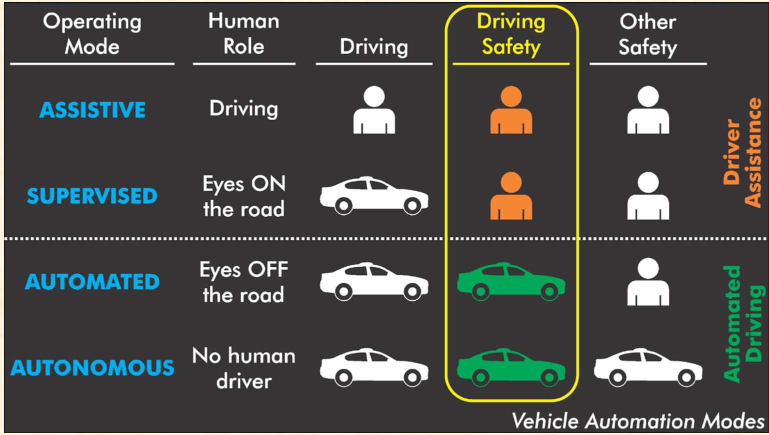
Autonomous: No Human Oversight

- Vehicle handles driving & vehicle safety
  - There is no driver; no human supervision
  - Ensures passenger & cargo safety
  - Handles non-driving issues (e.g., post-crash)

Shutterstock/
Metamorworks

- The vehicle is responsible safe operation
  - Human does not help with safety
  - OK for vehicle to get help if it initiates request all on its own
- Adds requirement for non-driving sensing (UL 4600)
  - Passenger safety; cargo safety; vehicle equipment status
  - Beyond scope of Automated Driving System Levels in J3016

Driver Roles Contrasted



Operating Mode	Human Role	Driving	Driving Safety	Other Safety	
ASSISTIVE	Driving	👤	👤	👤	Driver Assistance
SUPERVISED	Eyes ON the road	🚗	👤	👤	
AUTOMATED	Eyes OFF the road	🚗	🚗	👤	Automated Driving
AUTONOMOUS	No human driver	🚗	🚗	🚗	

Vehicle Automation Modes

Assistive & Supervised

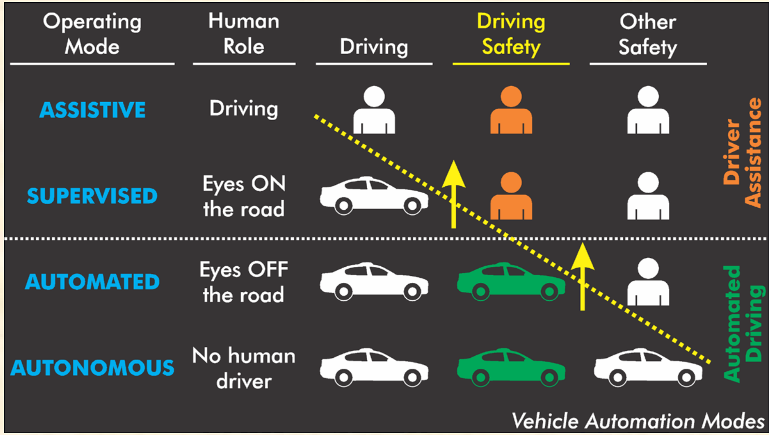
- Driver attention required
- Vehicle responds to driver
- Vehicle blame for unsafe intervention
  - – Incentive for vehicle to under-perform

Automated & Autonomous

- No human attention on driving
  - – Vehicle cannot count on human intervention for driving safety
- Mode changes are requests, not demands by vehicle
  - – Human actively confirms responsibility

Driver Mode Transitions

- Mode confusion is a problem
  - Driver positive acknowledgment
  - Request user attention, not “demand”
- Example issues:
  - Supervised changes to Assistive
    - Driver thinks vehicle is still steering
  - Automated changes to Supervised
    - Driver takes extended time to regain situational awareness
    - “Captain of ship” does not have a full driving license
  - Autonomous changes to Automated
    - Attendant rouses then falls back asleep (sleeps through alarm)



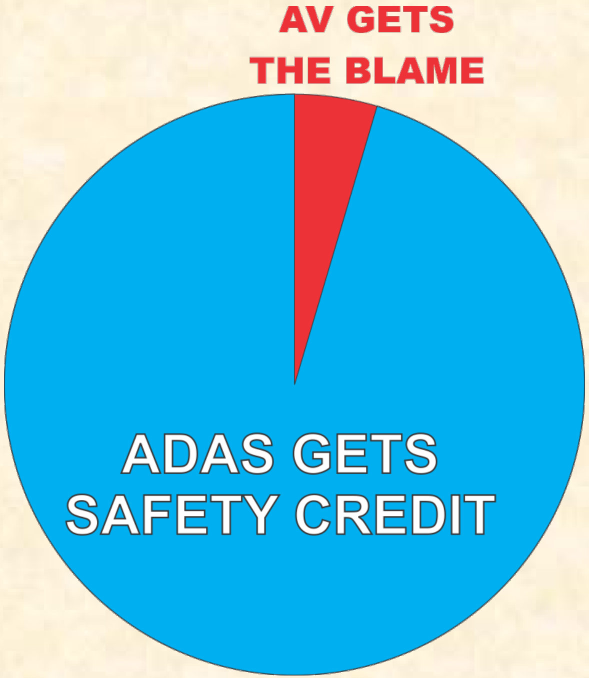
Operating Mode	Human Role	Driving	Driving Safety	Other Safety
ASSISTIVE	Driving	👤	👤	👤
SUPERVISED	Eyes ON the road	🚗	👤	👤
AUTOMATED	Eyes OFF the road	🚗	🚗	👤
AUTONOMOUS	No human driver	🚗	🚗	🚗

Vehicle Automation Modes

Automation Safety Challenges

Carnegie Mellon University

- Assistive
  - More uniform adoption of ISO 26262
- Supervised
  - Safety credit if low false positives
  - Effective driver monitoring
- Automated
  - SOTIF, scenario completeness & coverage
  - Sensor fusion, perception, prediction
  - Blamed for false negatives
- Autonomous
  - UL 4600 coverage: drivers do more than drive



Component Safety Challenges

- **Positive Trust Balance:**
  - Engineering Rigor, Validation, Feedback, Safety Culture
  - Standards-driven safety
- **Safety Performance Indicators (SPIs)**
  - Integrators asking for component safety cases
  - Field feedback: development; deployed
- **Scalability past pilot vehicles**
  - Accurate perception/prediction is still work in progress
  - Transition from brute force data to safety case
  - Key point: avoiding multi-sensor correlated failures

Edge Case Research

Organizational Safety Challenges

Carnegie Mellon University

- Significant pressure to deploy
  - Flurry of empty driver seat demos in 2020
  - Can teams take the time needed for safety?
- Industry transparency needed
  - Safety collaboration rather than competition
  - Public trust in face of an adverse news event
- Ensuring robust safety cultures
  - Robotics meets automotive engineering
  - Silicon Valley culture + automotive culture + no human driver

https://youtu.be/nhqyrze30bk
Yandex demo video, Ann Arbor, Aug 2020