Implications of Removing the Human Driver

Carnegie Mellon University

© 2021 Philip Koopman

Toyota "Unintended Acceleration" Has Killed 89

A 2005 Toyota Prius, which was in an accident, is seen at a police station in Harrison, New York, Wednesday, March 10, 2010. The driver of the Toyota Prius told police that the car accelerated on its own, then lurched down a driveway, across a road and into a stone wall. (AP Photo/Seth Wenig) / AP PHOTO/SETH WENIG

Unintended acceleration in Toyota vehicles may have been involved in the deaths of 89 people over the past decade, upgrading the number of deaths possibly linked to the massive recalls, the government said Tuesday.

The National Highway Traffic Safety Administration said that from 2000 to mid-May, it had received more than 6,200 complaints involving sudden acceleration in Toyota vehicles. The reports include 89 deaths and 57 injuries over the same period. Previously, 52 deaths had been suspected of being connected to the problem.

See: https://users.ece.cmu.edu/~koopman/toyota/index.html

It's All Your Fault: The DOT Renders Its Verdict on Toyota's Unintended-Acceleration Scare

The final word on the Toyota unintended-acceleration mess.

CSABA CSERE JUN 9, 2011

From the June 2011 issue of ***Car and Driver***

Tesla Blames Driver In Fatal Model X Autopilot Crash As Family Considers Legal Action

https://bit.ly/2m9cQRm

Justin T. Westbrook
4/11/18 8:00pm • Filed to: TESLA

84.6K 325 7

Huang fatality; crash into concrete median.

© 2021 Philip Koopman

Tesla car suddenly and unintentionally accelerated into driver's house, lawsuit says

Ji Chang Son says that Tesla's Model X vehicles are plagued by the phenomenon

Amy Martyn
Reporter

Feds blame driver error for 16,000 annual unintended acceleration cases

Accident victims don't buy the argument but few can document any other cause

James R. Hood
Founder and Editor

Peggy's Jeep

Can Humans Safely Supervise Autonomy?

Carnegie Mellon University

Man reportedly caught sleeping behind the wheel of a self-driving Tesla

https://goo.gl/ZFCYzD

Sarah Whitten | @sarahwhit10

Published 11:38 AM ET Wed, 25 May 2016 | Updated 9:46 AM ET Thu, 26 May 2016

CNBC

Google's Waymo Self-Driving Car Crashed After Driver Dozed Off Back in June

Justin T. Westbrook

10/04/18 10:28am • Filed to: WAYMO

JALOPNIK

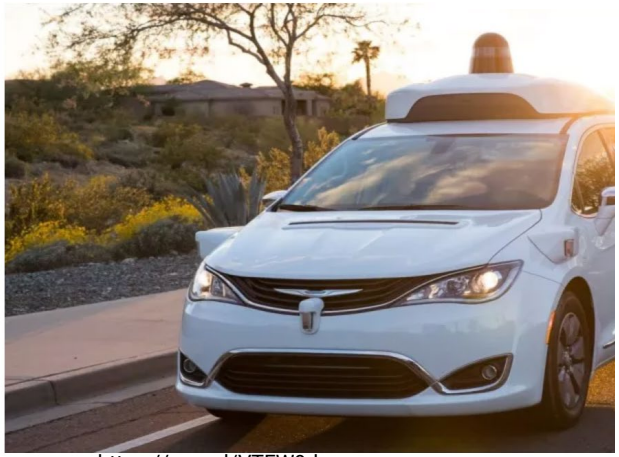


Photo: Waymo https://goo.gl/VTFW9d

A Waymo self-driving car sent a motorcyclist to the hospital — but the human driver was at fault

BUSINESS INSIDER

Graham Rapier Nov. 6, 2018, 4:20 PM

Waymo https://goo.gl/kgRq71

The 94% Human Error False Narrative

Carnegie Mellon University

- Where did "94%" come from?

"94%"

  - "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."

    [DOT HS 812 115]

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

- Looking a little deeper:
  - 74% of driver errors were "recognition" or "decision" errors
  - And software driver must handle the 6% of no-driver-involvement crash causes
    - Tires, brakes, drivetrain failures

© 2021 Philip Koopman

Humans Are Amazing Fault Mitigators

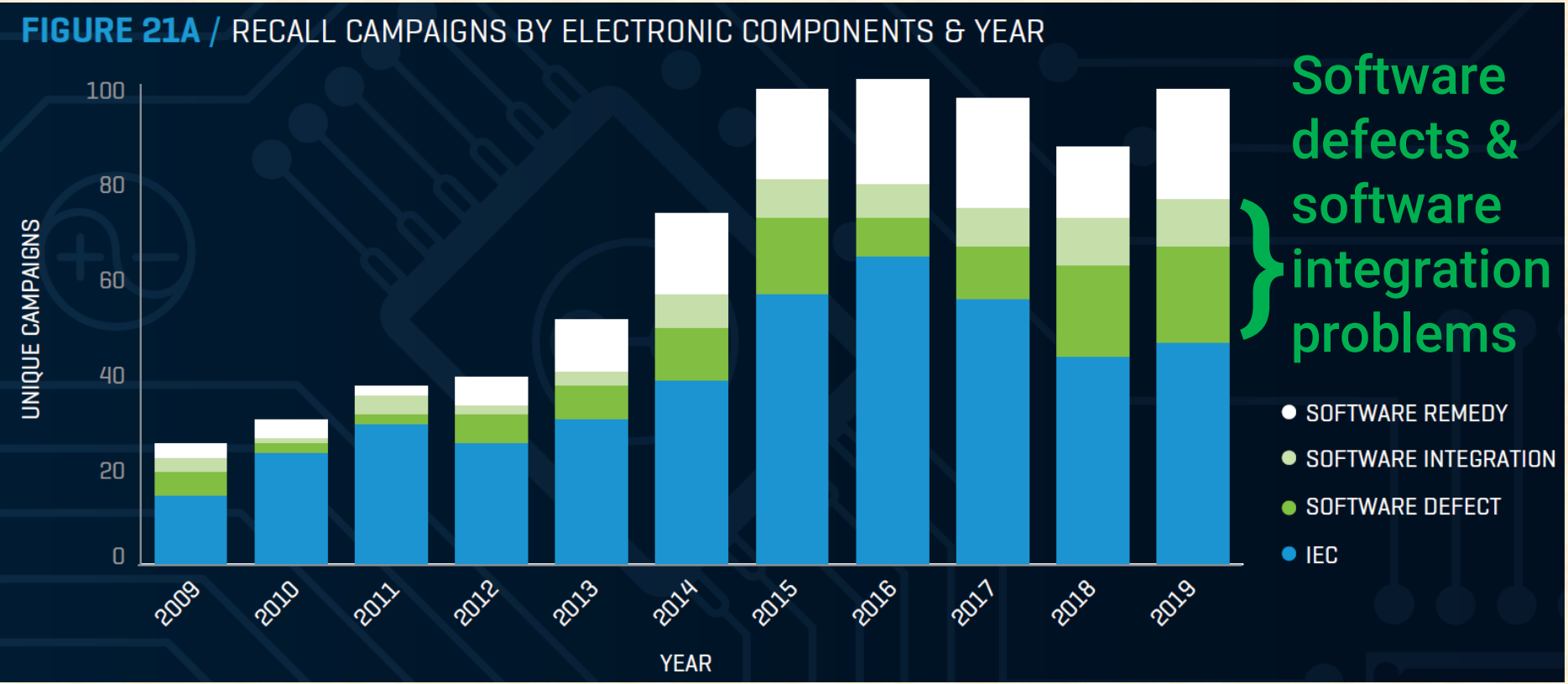
Carnegie Mellon University

- Other side of the "94%" coin – people prevent crashes too
- Toyota uncommanded acceleration – most saved by human
  - 89 deaths, 57 injuries as of May 2010
  - 6,200+ NHTSA complaints [https://www.cbsnews.com/news/toyota-unintended-acceleration-has-killed-89/]
- GM brake issues – most saved by human
  - 293 injuries, 2111 crashes
  - 10,861 NHTSA complaints https://www.nytimes.com/1999/07/22/us/gm-admits-brake-flaws-after-inquiry.html
- Will an ADS be as successful at fault mitigation as humans?
  - ADS will need to deal with heavy-tail issues

© 2021 Philip Koopman

Automotive Software Quality Issues

Carnegie Mellon University



Source: Stout 2020 Automotive Defect & Recall Report
IEC is integrated electronic components (hardware)

© 2021 Philip Koopman

Automotive Software Has Defects

Carnegie Mellon University

- **Small sampling of NHTSA recalls (i.e., confirmed bugs)**
  - See: https://betterembsw.blogspot.com/p/potentially-deadly-automotive-software.html
  - 21V-071 Vehicle unexpected pulls to one side during evasive maneuver
  - 20V-213 Remote smart park continued motion after failsafe activation
  - 19E-070 Anti-rollback software causes unexpected vehicle motion
  - 19V-539 Forward collision avoidance does not detect stationary vehicle
  - 19V-351 Regenerative braking failure reduces deceleration
  - 19V-075 Transmission unexpected downshift to first gear causes loss of control
  - 18V-621 Automatic braking cancelled / ABS locks up wheels
  - 18V-607 Active Lane Keeping Assist does not intervene in lane departure
  - 17V-713: Engine does not reduce power due to ESP software defect
  - **17V-686 *and MANY others*: Airbags disabled**
  - **15V-460 *and others*: Airbags deploy when they should not**

© 2021 Philip Koopman

Example Required ADS Fault Handling

Carnegie Mellon University

- Tire blowout/wheel detachment
  - ADS: perform controlled stop (or run-flat tire operations)
- Service brake failure
  - ADS: downshift/regen braking, apply parking brake, runaway ramp
- Catastrophic sensor failure
  - ADS: dead reckon to stop using most recent object trajectories
- Uncommanded acceleration
  - ADS: de-energize engine/motors, apply forceful brakes
- Main battery fire
  - ADS: shed electrical load, stop vehicle, passenger evacuation

© 2021 Philip Koopman

Controllability Without A Human Driver

Carnegie Mellon University

- What happens when there is no human to exert controllability?
  - Own vehicle human driver?
  - Other vehicle human driver?
- Some combination of:
  - ADS will need to control faults to attain C1 or C2
  - Vehicle will have to upgrade subsystems to C3 (“uncontrollable”)
- Potential for significant ASIL increase across whole vehicle
  - Many ADS control requirements

Severity class	Exposure class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	?	A
	E4	QM	?	B
S2	E1	QM	?	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	?	B	C
S3	E1	?	QM	A[a]
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

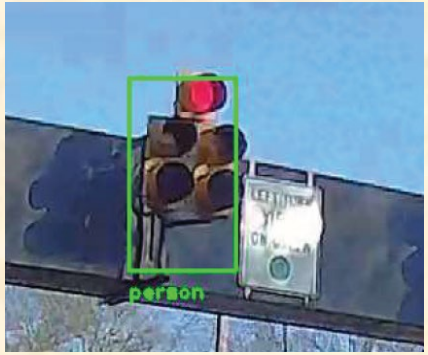
- ISO 26262 Driver Controllability:
  - C1 = Simply controllable
  - C2 = Normally controllable
  - C3 = Difficult / uncontrollable

© 2021 Philip Koopman

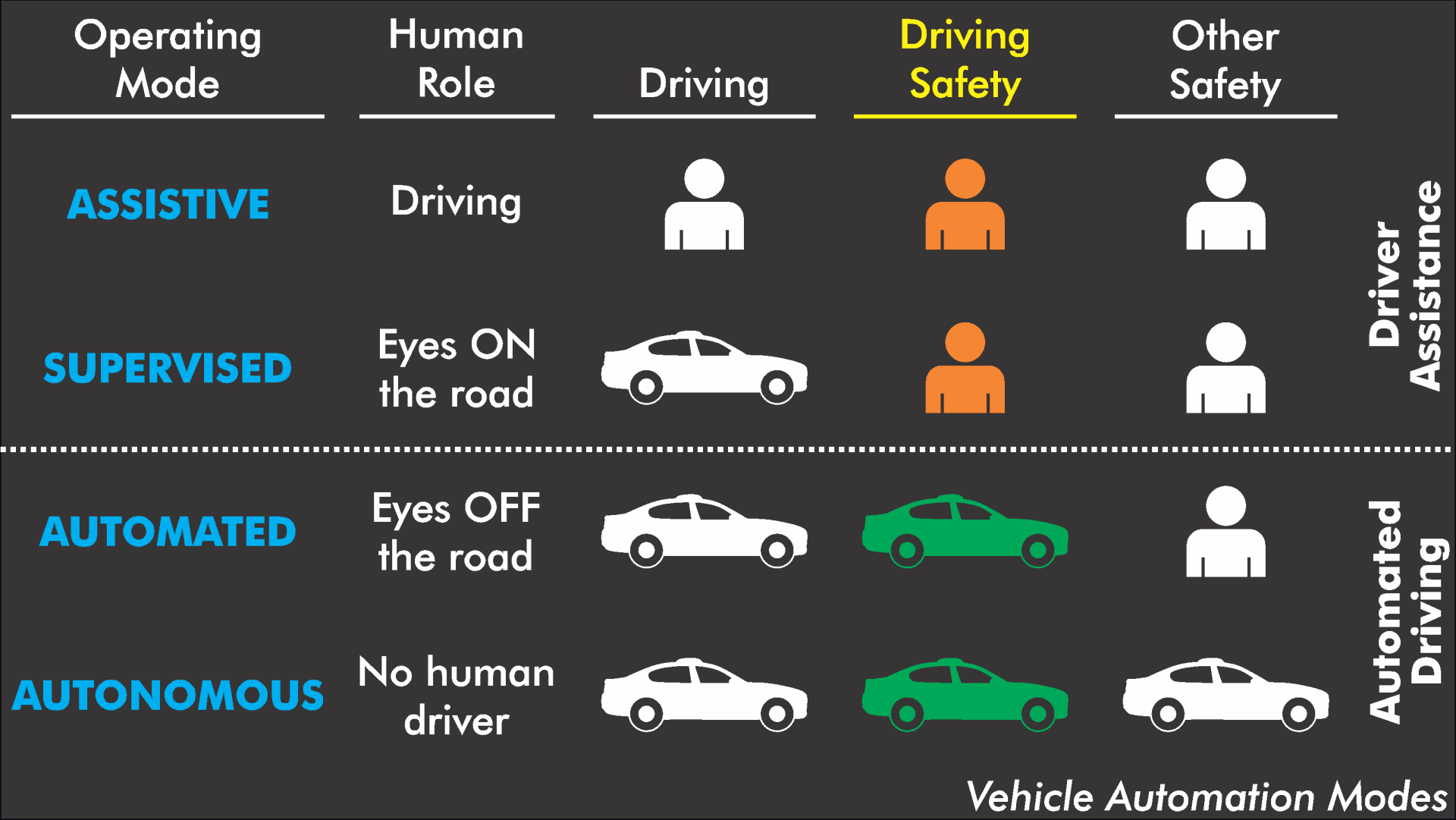
No Human Driver to Blame

Carnegie Mellon University

- "Computers won't drive drunk" .. but …
  - Drunk/DUI is only 28% of fatalities (US 2019)
    [https://crashstats.nhtsa.dot.gov/Api/Public/Publication/813060]
  - Automated Driving Systems (ADS) will likely make *different* mistakes
    - Perception/classification errors
    - Brittle in face of surprises (unknown unknowns)
- What happens with ADS "driver error"?
  - Every AV crash is a product liability lawsuit waiting to happen
  - Eventually, no human driver to absorb blame
    - What about Driver monitor system (DMS) failures?



© 2021 Philip Koopman


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
Driver Assistance
Automated Driving
Vehicle Automation Modes

Operations & Human Interactions

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
  - Vehicle fire or catastrophic failure
  - Post-crash response
- Interacting with non-drivers
  - Pedestrians, passengers
  - Police, emergency responders


https://bit.ly/2GvDkUN


https://bit.ly/2PhzilT

Lifecycle Issues

- Handling updates
  - Fully recertify after every weekly update?
  - Security in general
- Vehicle maintenance
  - Pre-flight checks, cleaning
  - Corrective maintenance
- Supply chain issues
  - Quality fade
  - Supply chain faults

Is windshield cleaning fluid life critical?

© 2021 Philip Koopman

Changing Role of Human Driver

- No human driver to blame for crashes
- ADS handles vehicle equipment failures
- ADS handles non-ADS software failures

Carnegie Mellon University

© 2021 Philip Koopman