Prof. Philip Koopman

Current State of Automotive Software Safety

ASSC; 22 May 2019

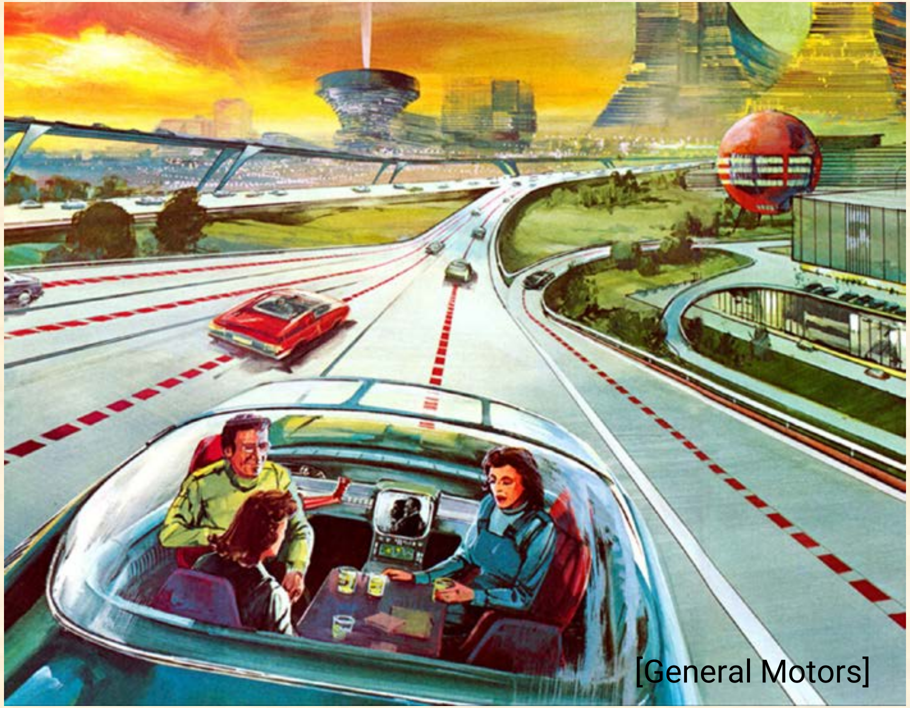
Carnegie Mellon University

@PhilKoopman

Electrical & Computer ENGINEERING

Overview

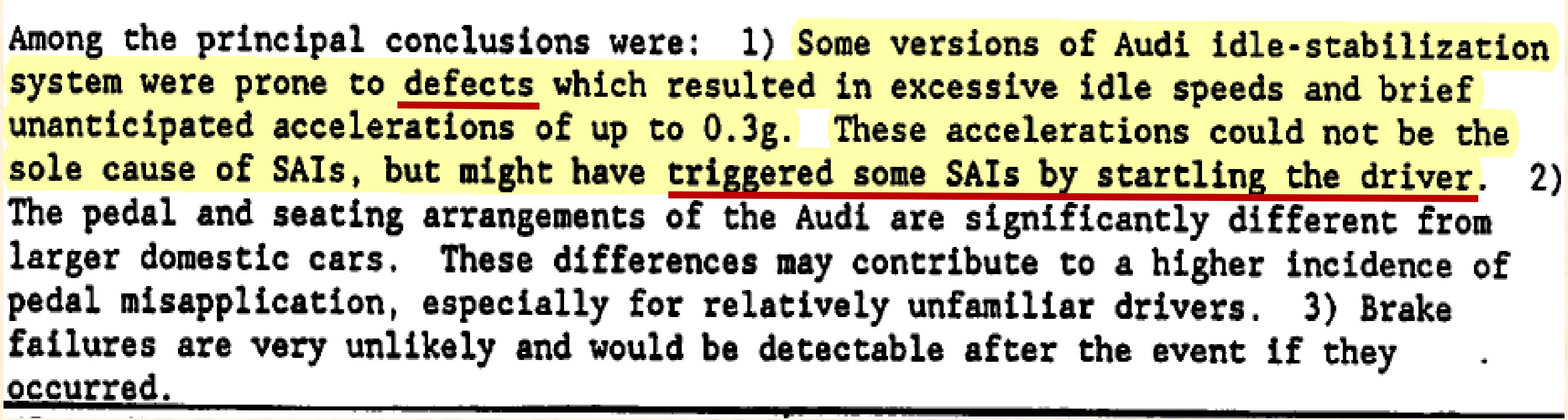
- **"It's the driver's fault"**
  - Yes, there are safety critical defects in cars!
  - The pedal misapplication narrative
- **Taking Stock**
  - How good is automotive software safety right now?
  - How will the "94%" narrative work out for self-driving car safety?



[General Motors]

Birth of the Pedal Misapplication Narrative

- **Audi 5000: before full authority computer throttle control**
  - Public narrative: driver pedal mis-application & pedal placement



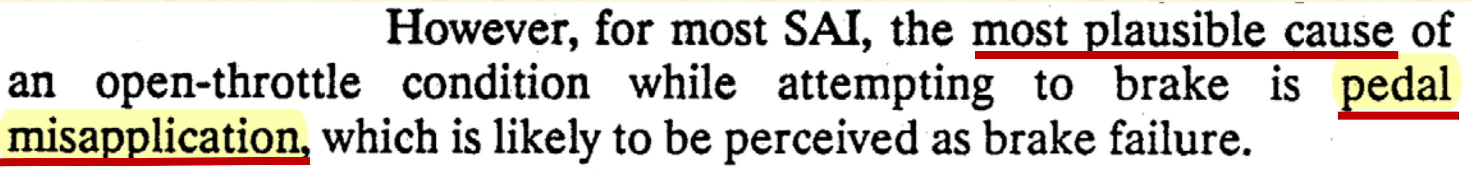
Among the principal conclusions were: 1) Some versions of Audi idle-stabilization system were prone to defects which resulted in excessive idle speeds and brief unanticipated accelerations of up to 0.3g. These accelerations could not be the sole cause of SAIs, but might have triggered some SAIs by startling the driver. 2) The pedal and seating arrangements of the Audi are significantly different from larger domestic cars. These differences may contribute to a higher incidence of pedal misapplication, especially for relatively unfamiliar drivers. 3) Brake failures are very unlikely and would be detectable after the event if they occurred.

Pollard & Sussman, 1989, DOT-TSC-NHTSA-88-4 Appendix H; 1983-85 Audi 5000

Note: 0.3g is 0-to-60mph in 9.1 seconds; 1983 Audi 5000S 0-60 track time is 10.7 sec.

https://www.zeroto60times.com/vehicle-make/audi-0-60-mph-times/

"It's the Drivers' Fault"

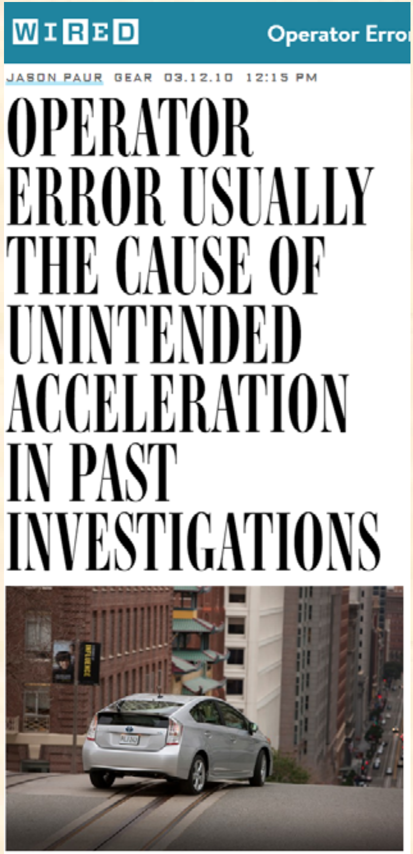


However, for most SAI, the most plausible cause of an open-throttle condition while attempting to brake is pedal misapplication, which is likely to be perceived as brake failure.

- Pollard & Sussman, **1989** – *the same Audi 5000 report!*

- **~"Most crashes are due to human error, therefore all unexplained crashes are due to human driver error"~**
  - *Note: this is clearly a logical fallacy*
  - NHTSA reports fail to rule in software as a possible cause
- **Investigations:**
  - No mechanical cause found ➔ driver error
    - Compelling facts supporting human results in "unexplained"
  - Non-reproducible behavior ➔ driver error
  - "Pedal Misapplication" often blamed

2010



WIRED Operator Erro

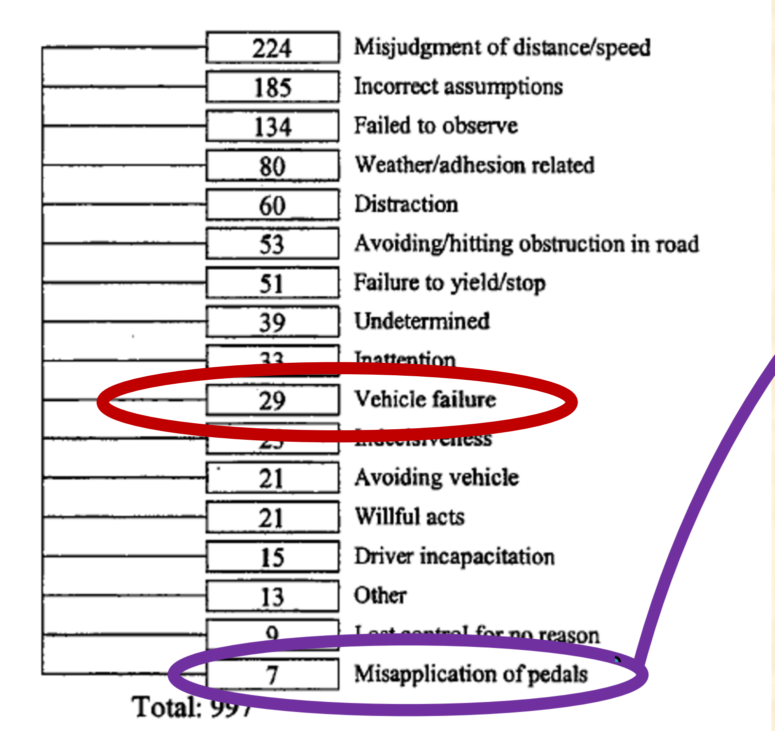
JASON PAUR GEAR 03.12.10 12:15 PM

OPERATOR ERROR USUALLY THE CAUSE OF UNINTENDED ACCELERATION IN PAST INVESTIGATIONS

https://www.wired.com/2010/03/unintended-acceleration/

Actual Pedal Misapplication Data

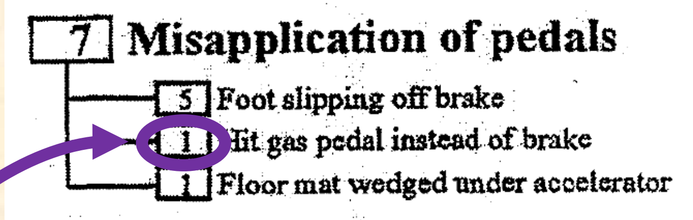
- **Gas/Brake confusion about 0.1% of crashes** (Pre-ETC data)



224	Misjudgment of distance/speed
185	Incorrect assumptions
134	Failed to observe
80	Weather/adhesion related
60	Distraction
53	Avoiding/hitting obstruction in road
51	Failure to yield/stop
39	Undetermined
33	Inattention
29	Vehicle failure
23	Indecisiveness
21	Avoiding vehicle
21	Willful acts
15	Driver incapacitation
13	Other
9	Lost control for no reason
7	Misapplication of pedals

Total: 997

Figure A27b. Reason/excuses taxonomy.



7 Misapplication of pedals

5	Foot slipping off brake
1	Hit gas pedal instead of brake
1	Floor mat wedged under accelerator

- **Other data supports this**
- **Some reports cite high rates of pedal confusion, *but*:**
  - Based on inability to replicate fault
  - Based on news & police reports
    - Police don't consider software defects

Wierwille at al., FHWA-RD-02-003, **2002**

Toyota Unintended Acceleration

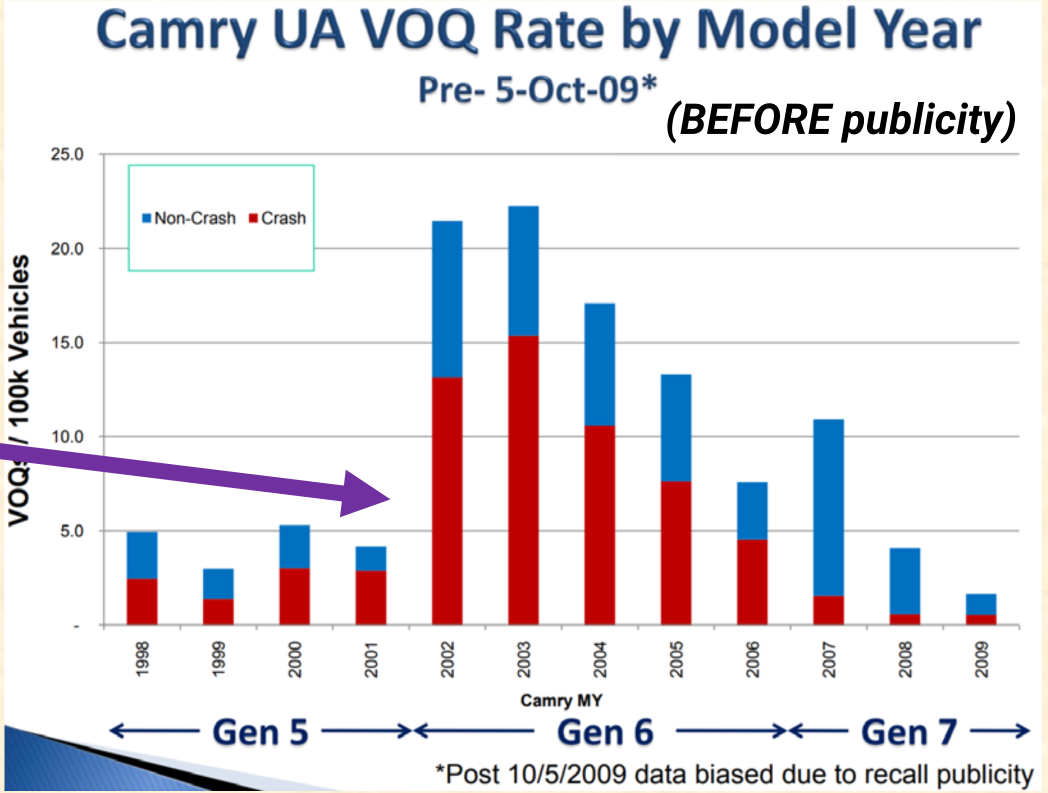
- **The only public trial found in favor of Plaintiffs**
  - 500+ death and injury settlements

Introduction of Full Authority Electronic Throttle Control (ETC)

  - What changed in 2002?

Full talk at https://goo.gl/fXrErn

NHTSA slide from 2010 / Owner UA complaint rates



Camry UA VOQ Rate by Model Year

Pre- 5-Oct-09*

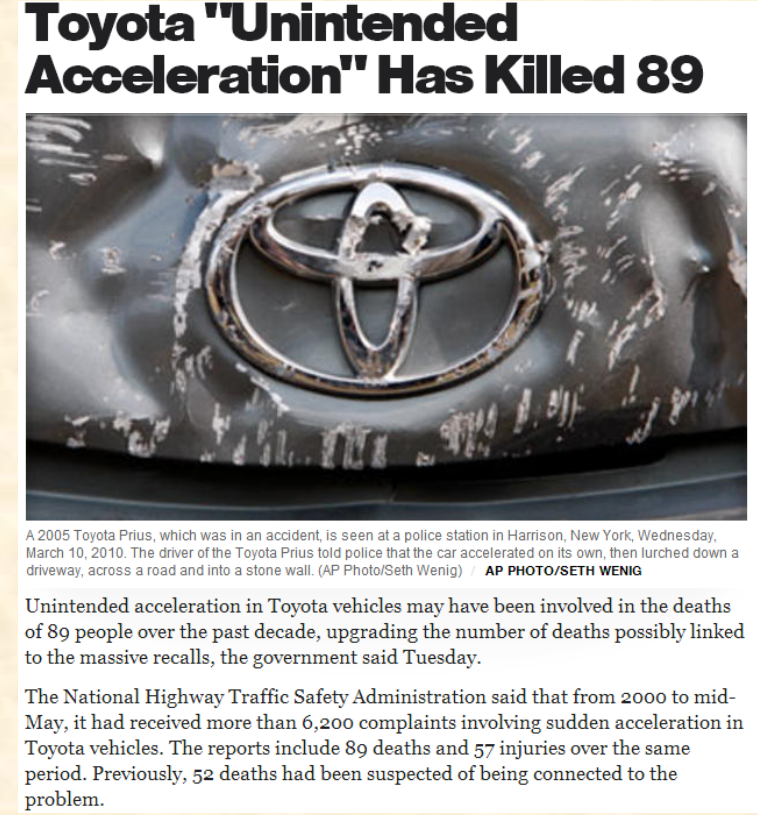
(BEFORE publicity)

*Post 10/5/2009 data biased due to recall publicity

http://onlinepubs.trb.org/onlinepubs/ua/100630DOTSlides.pdf

US Government Position on Toyota UA

- **DOT Claims no electronics/software fault**
  - "No evidence of an electronic defect in Toyota vehicles capable of producing dangerous, high-speed unintended acceleration incidents"
  - (What NASA *actually said* was they couldn't find a smoking gun; litigation expanded scope)
- **Recalls for safety defects**
  - Pedal floor mat entrapment
  - Sticking accelerator pedals
  - Criminal fine of $1.2B for Toyota cover-up
- **Emphasize reducing pedal mis-application**



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

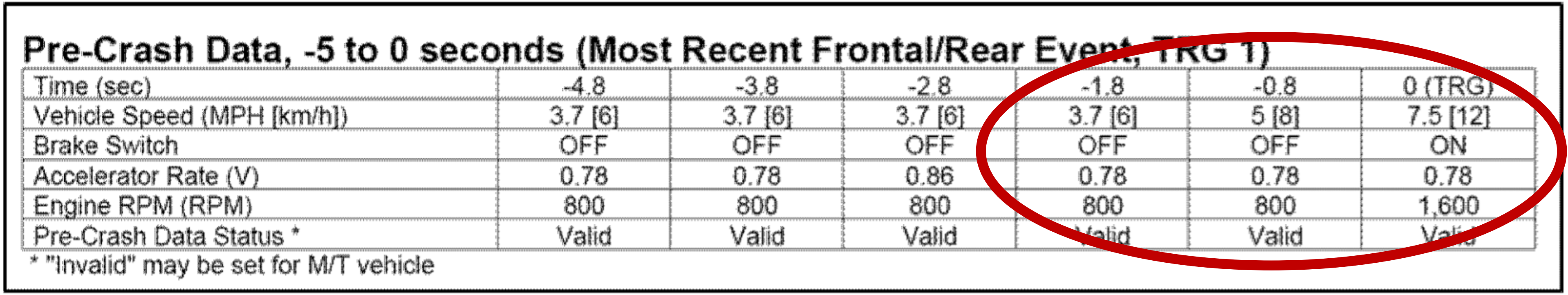
Unintended acceleration in Toyota vehicles may have been involved in the deaths of 89 people over the past decade, upgrading the number of deaths possibly linked to the massive recalls, the government said Tuesday.

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.

http://www.cbsnews.com/news/toyota-unintended-acceleration-has-killed-89/

Source: https://www.transportation.gov/briefing-room/us-department-transportation-releases-results-nhtsa-nasa-study-unintended-acceleration

Ruginis Vehicle EDR Data Analysis (2015)



Pre-Crash Data, -5 to 0 seconds (Most Recent Frontal/Rear Event, TRG 1)

Time (sec)	-4.8	-3.8	-2.8	-1.8	-0.8	0 (TRG)
Vehicle Speed (MPH [km/h])	3.7 [6]	3.7 [6]	3.7 [6]	3.7 [6]	5 [8]	7.5 [12]
Brake Switch	OFF	OFF	OFF	OFF	OFF	ON
Accelerator Rate (V)	0.78	0.78	0.86	0.78	0.78	0.78
Engine RPM (RPM)	800	800	800	800	800	1,600
Pre-Crash Data Status *	Valid	Valid	Valid	Valid	Valid	Valid

* "Invalid" may be set for M/T vehicle

2010 Toyota Corolla Federal Register v. 80 n. 93 pg. 27835-27844, May 2015

- **Petitioner: consider -1.8 seconds to 0 seconds (crash)**
  - Repeated surge complaints to dealer; engine speed doubles; vehicle speed doubles
  - Accelerator pedal position constant (idle); Brake has been applied at/before crash
- **NHTSA denied investigation request:**
  - “Driver statements regarding pedal use in such incidents are not reliable”
  - Extensive critique of Barr Group analysis & other crash EDR data analysis
  - Finding: Brakes are functional, so driver must not have applied meaningful braking
  - Finding: driver pumped accelerator and then pressed brake within 0.8 sec

Current US Regulatory Strategy

- **US Govt regulates technology**
  - State governments regulate/license drivers
  - Regulators have minimal software expertise
  - **Vehicle makers self-certify**

FMVSS 138 Telltale

- **Safety primarily via vehicle tests**
  - FMVSS: Federal Motor Vehicle Safety Standards
  - Emphasizes vehicle safety functions (e.g., brakes)
  - No requirement for software safety

- **Reactive safety – recalls & litigation**

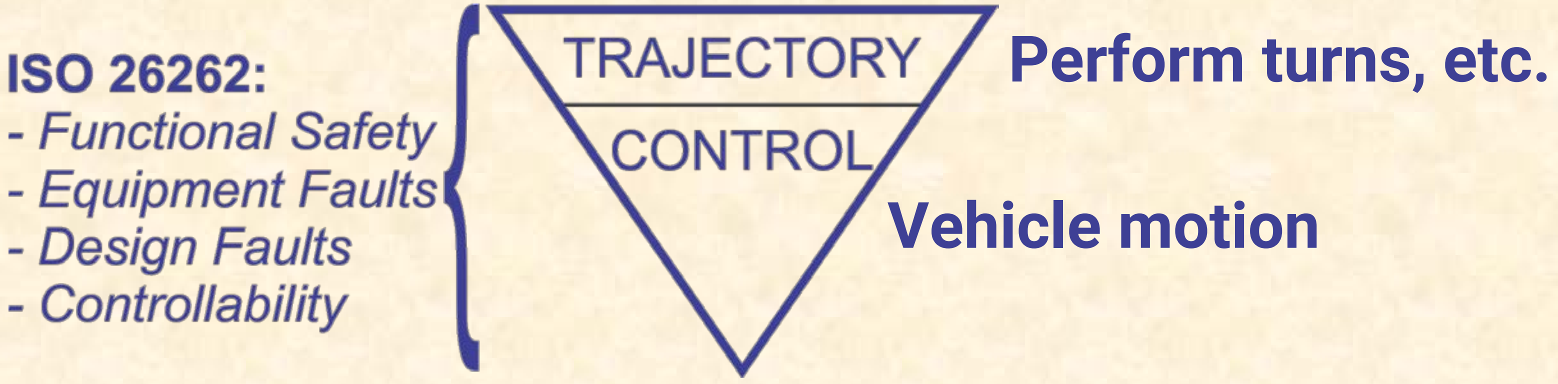
Common Car Industry Approaches

- **Design to internal standards**
  - Potentially less than ISO 26262
- **Primarily system-level testing**
  - Validation via accumulating miles
- **Focus on reproducible defects**
  - Neglect "unrealistic" faults
  - Don't chase non-reproducible defects
  - Blame drivers for transient field failures
- **Declare "safe" if all known, reproducible defects are fixed**
  - Self-certification, not independent assessment

YouTube: PknOqXqcnUo, M1XHjl_6HtM, -0hE6gAcbvg, y6Krr4TazMg

Conventional Vehicle Safety

- **Human driver ultimately responsible for safety**
  - "**Functional Safety**" – respond to equipment; avoid design faults
  - Human does the right thing for malfunctions ("Controllability")



ISO 26262:

- *Functional Safety*
- *Equipment Faults*
- *Design Faults*
- *Controllability*

Perform turns, etc.

Vehicle motion

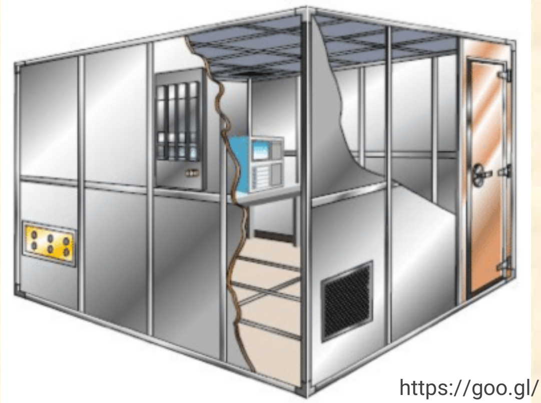
Example Automotive Software Defects

- ***Small*** **sampling of NHTSA recalls (i.e., confirmed bugs)**
  - 17V-713: Engine does not reduce power due to ESP software defect
  - 17V-686 *and MANY others*: Airbags disabled
  - 15V-569: Unexpected steering motion causes loss of control
  - 15V-460 *and others*: Airbags deploy when they should not
  - 15V-145: Unattended vehicle starts engine → carbon monoxide poisoning
  - 14V-370: Turns off headlights when driving
  - 14V-204: 1.5 seconds reverse while displaying Drive

  Voluntary Recalls:
  - 2018 hybrid engine stall at high speeds (https://bloom.bg/2y21T71)
  - 2014 sudden unintended acceleration (https://goo.gl/R9zgL1)

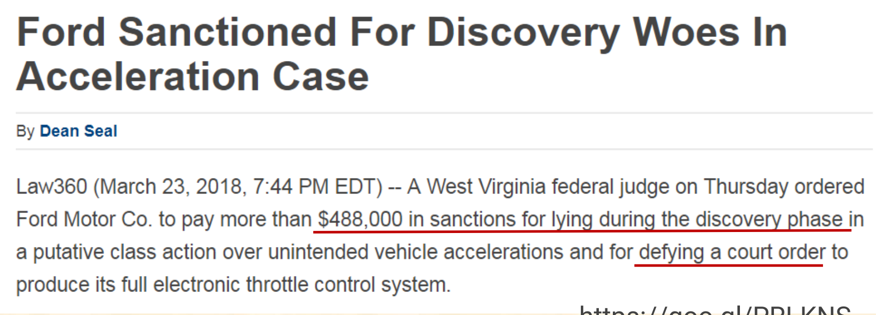
Practical Aspects of Recalls & Litigation

- **Recalls based on statistical evidence of faults**
  - There have to be victims and/or reports
  - NHTSA does not do software analysis
  - Relies heavily on truthful OEM statements
- **Litigation is expensive and difficult**
  - Access conditions are difficult
  - Expensive: >$1M to analysis campaign
    - Many cases are just too small to afford this
  - Economic & legal outcome uncertain
    - You can't make a nondeterministic bug perform on demand via system test
    - Experts paid win or lose



https://goo.gl/RQi1ik

(Not the actual Toyota source code room)



Ford Sanctioned For Discovery Woes In Acceleration Case

By **Dean Seal**

Law360 (March 23, 2018, 7:44 PM EDT) -- A West Virginia federal judge on Thursday ordered Ford Motor Co. to pay more than $488,000 in sanctions for lying during the discovery phase in a putative class action over unintended vehicle accelerations and for defying a court order to produce its full electronic throttle control system.

https://goo.gl/PRLKNS

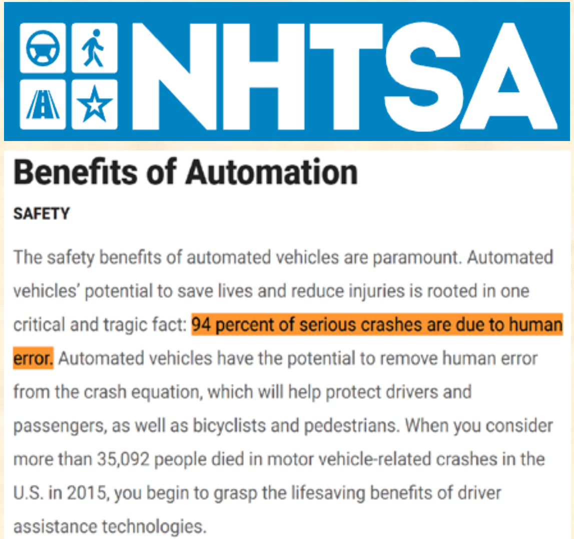
Why Does Society Want Self Driving Cars?

- **Where did “94%” come from?**
  - “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]

“94%”



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

- **Practical improvement perhaps only 50%**
  - Casualty Actuarial Society, 2014 https://bit.ly/2IIXj3L

It’s Not All Cell Phone Distraction

U.S. Department of Transportation
National Highway Traffic Safety Administration

TRAFFIC SAFETY FACTS

Research Note

NHTSA

(2017 data DOT HS-812-603)

- **37,133 Fatalities**
  - 63% Passenger vehicles
  - 14% Motorcycles
  - 19% Pedestrians, bikes, etc.
  - 2% Large trucks (+ 2% other = 100%)
- **One fatality per 86 million miles, including impaired drivers**
  - 29% Alcohol Impairment
  - 27% Seat belt not used in passenger vehicle
  - 26% Speed (can be too fast for conditions)
  - 9% Distracted driving (total of all sources was more than 100% due to overlap)
- **The bar is set high for unimpaired humans**
  - 99.999999%+ fatality-free miles

Regulation & Standardization

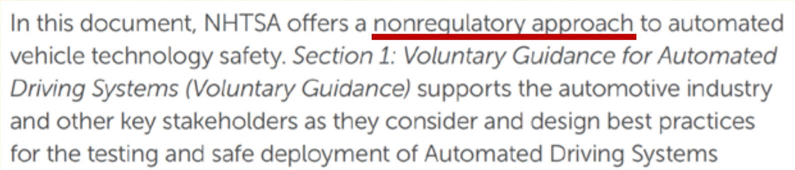
- **US DOT/NHTSA**
  - Economic incentives & self-certification
  - Encourage safety self-reports
  - No required software safety standard
- **US States & road testing**
  - Mostly registration & incident reports
- **Standards in flux**
  - SOTIF (ISO PAS 21448) for ADAS
  - New: UL 4600 for high autonomy
  - Others in progress (e.g., IEEE P7009)

AUTOMATED DRIVING SYSTEMS 2.0

A Vision for Safety

U.S. Department of Transportation

NHTSA

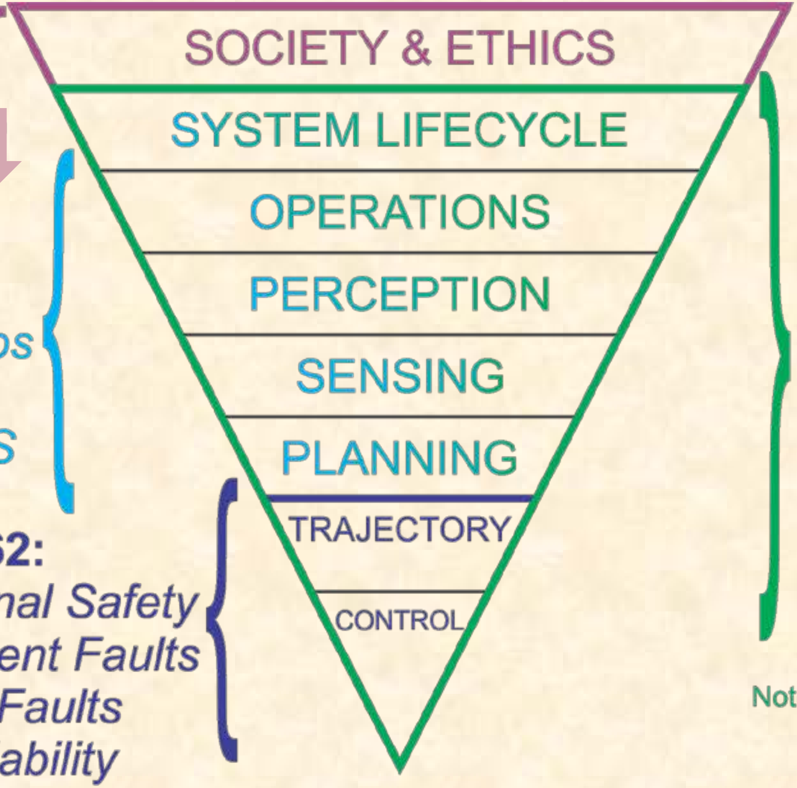


In this document, NHTSA offers a nonregulatory approach to automated vehicle technology safety. *Section 1: Voluntary Guidance for Automated Driving Systems (Voluntary Guidance)* supports the automotive industry and other key stakeholders as they consider and design best practices for the testing and safe deployment of Automated Driving Systems

https://goo.gl/GdAtt7

Safety Standard Landscape

IEEE P700x
- *Ethical Life-Cycle*



SOCIETY & ETHICS

SYSTEM LIFECYCLE

OPERATIONS

PERCEPTION

SENSING

PLANNING

TRAJECTORY

CONTROL

ISO 21448 (SOTIF):
- *Enumerate Scenarios*
- *Triggering Events*
- *Historically for ADAS*

ISO 26262:
- *Functional Safety*
- *Equipment Faults*
- *Design Faults*
- *Controllability*

Note: ISO 26262 covers functional safety lifecycle activities.

UL 4600: (Draft Scope)
- *Machine Learning Faults*
- *External Operational Faults*
- *Non-Driver Human Faults*
- *Nondeterminism*
- *High Residual Unknowns*
- *Field Feedback and Updates*
- *Lack of Human Oversight*
- *System-Level Safety Metrics*
- *Full Autonomous Driving: Excludes Human Supervision*

Note: Provides significantly more detailed treatment regarding autonomous systems for those topics also mentioned in ISO 21448, ISO 26262. Intended to supplement, not replace these.

To Dig Deeper

- Suggest you *follow the links* from the paper
  - https://users.ece.cmu.edu/~koopman/pubs/koopman18_safecomp.pdf

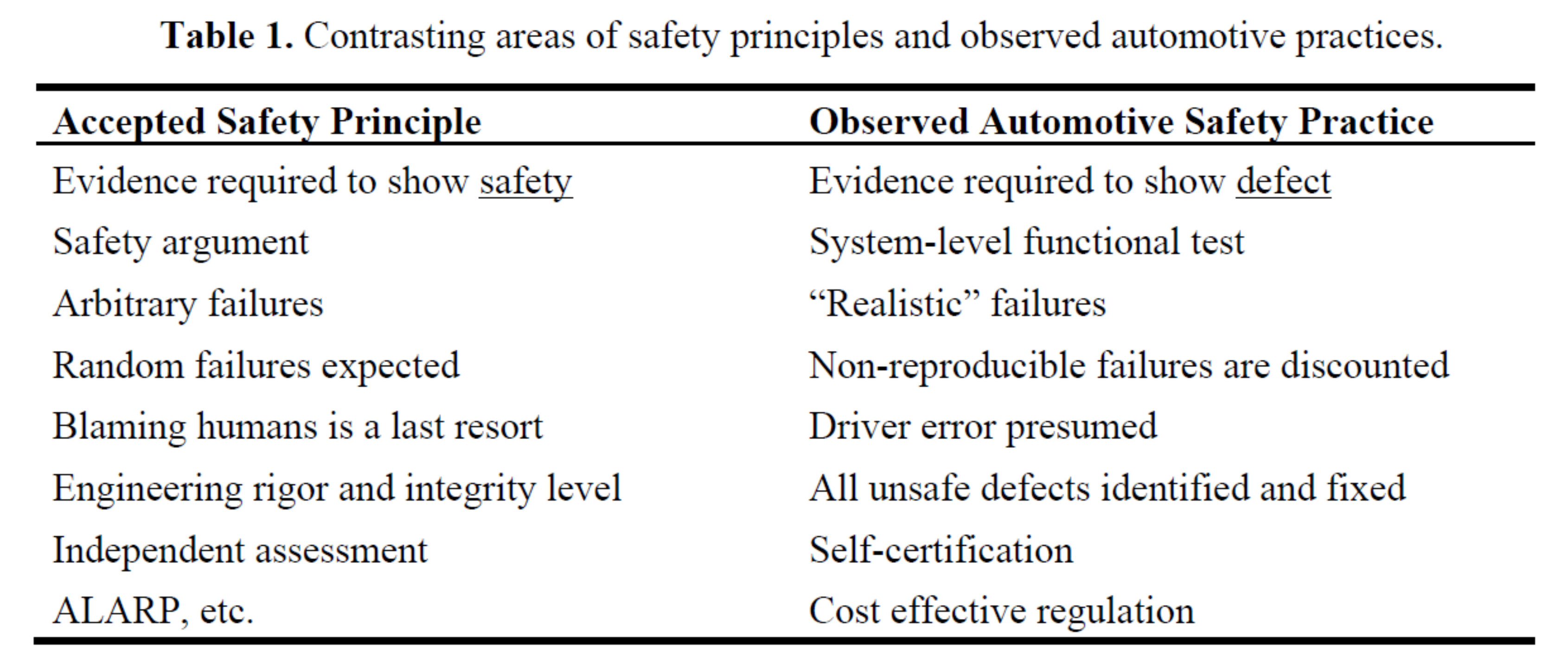


Table 1. Contrasting areas of safety principles and observed automotive practices.

Accepted Safety Principle	Observed Automotive Safety Practice
Evidence required to show safety	Evidence required to show defect
Safety argument	System-level functional test
Arbitrary failures	“Realistic” failures
Random failures expected	Non-reproducible failures are discounted
Blaming humans is a last resort	Driver error presumed
Engineering rigor and integrity level	All unsafe defects identified and fixed
Independent assessment	Self-certification
ALARP, etc.	Cost effective regulation