Automotive Safety Practices vs. Accepted Principles

SAFECOMP, Sept. 2018

Prof. Philip Koopman

Carnegie Mellon University

Electrical & Computer ENGINEERING

Overview

Carnegie Mellon University

- **"It's the driver's fault"**
  - Yes, there are safety critical defects in cars!
  - The pedal misapplication narrative
- **Regulations & litigation**
  - A cautionary tale for academics
- **A very brief look ahead**


[General Motors]

Example Automotive Software Defects

Carnegie Mellon University

- ***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-522: Disables brake power assist
  - 14V-395: Airbag disabled due to EEPROM wearout
  - 14V-370: Turns off headlights when driving
  - 14V-204: 1.5 seconds reverse while displaying Drive
  - 06V-007: Torque monitor UA failsafe disabled
  - https://goo.gl/R9zgL1: sudden unintended acceleration (voluntary recall)
  - https://goo.gl/NUQTzt: one second lag in braking (voluntary recall)

The Pedal Misapplication Narrative

Carnegie Mellon University

- **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"

Carnegie Mellon University

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 Error

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

Carnegie Mellon University

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

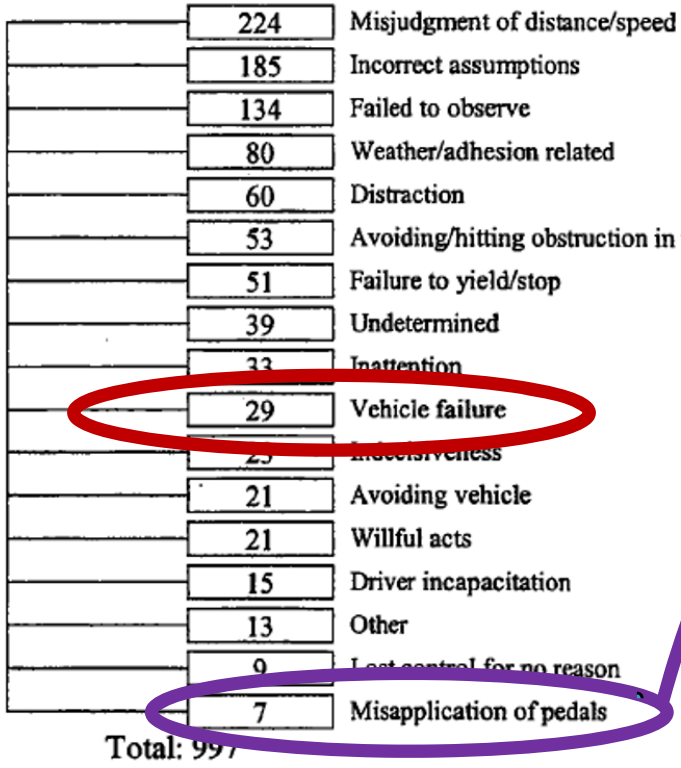
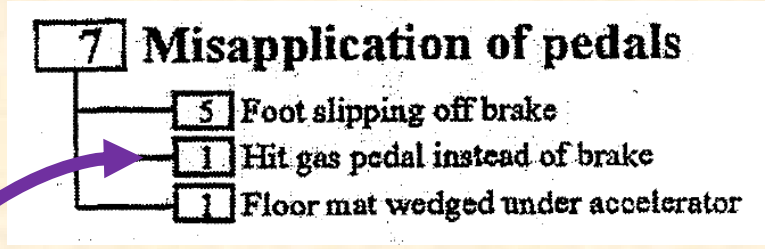


Figure A27b. Reason/excuses taxonomy.



- **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

Carnegie Mellon University

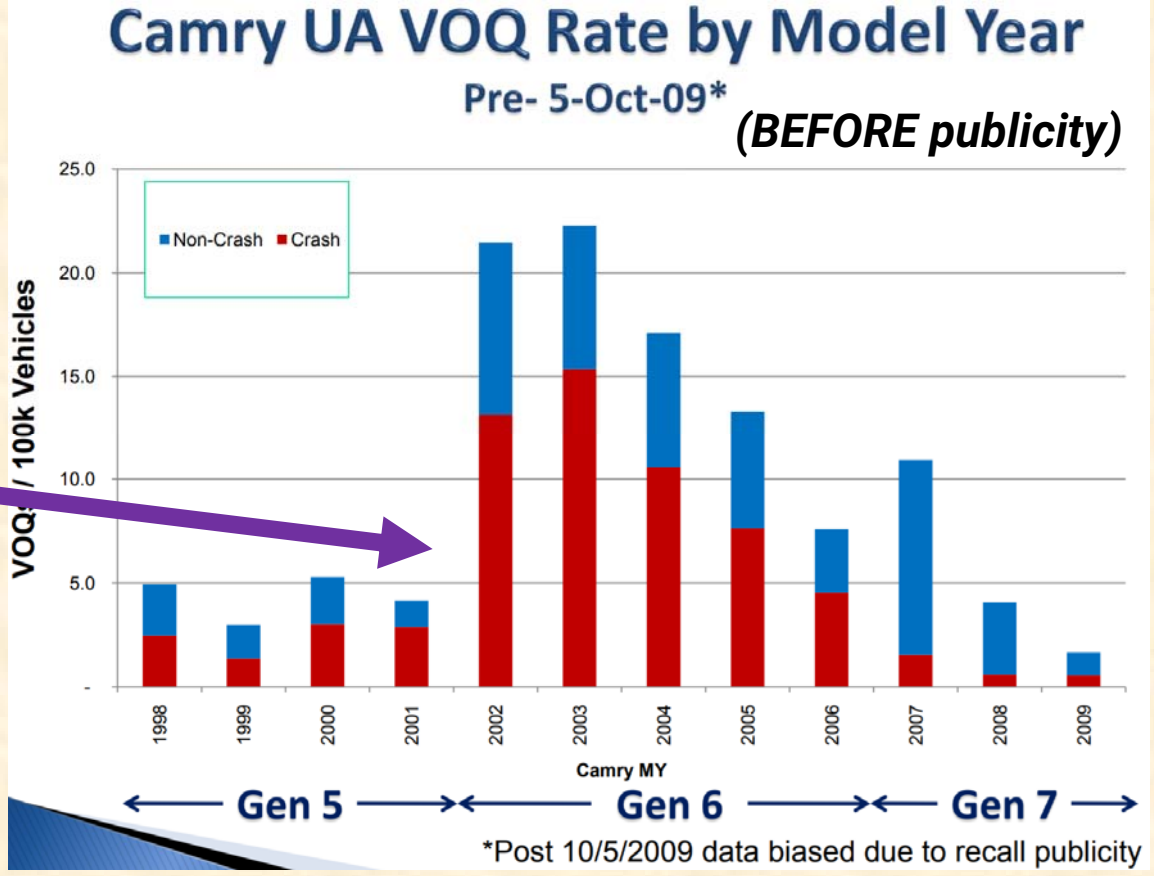
- **The only public trial found in favor of Plaintiffs**
  - 500+ death and injury settlements

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



US Government Position on Toyota UA

Carnegie Mellon University

- **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)

Carnegie Mellon University

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

Common Car Industry Approaches

Carnegie Mellon University

- **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

Current US Regulatory Strategy

Carnegie Mellon University

- **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**

Practical Aspects of Recalls & Litigation

Carnegie Mellon University

- **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

And Now: Self Driving Cars

Carnegie Mellon University

- **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)

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

A Cautionary Tale for Academics

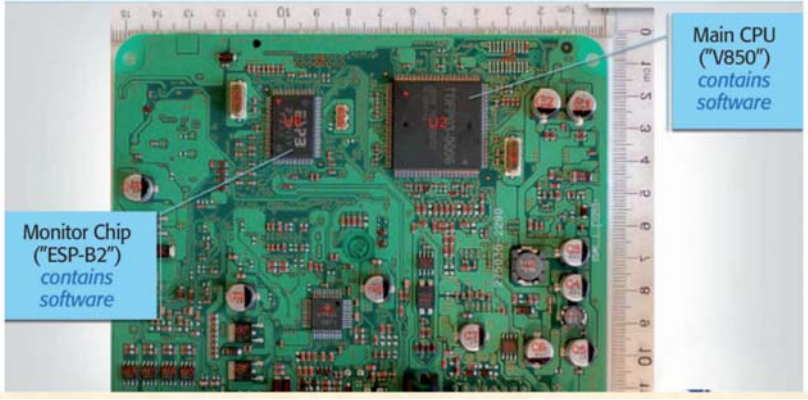
Carnegie Mellon University

December 2016

Embedded Software Under the Courtroom Microscope

A Case Study of the Toyota Unintended Acceleration Trial

TOYOTA'S ENGINE CONTROL MODULE (ECM)



GOOD-BAD © CANSTOCK PHOTO/STUARTMILES, CHIP COURTESY OF FREEIMAGES.COM/DIMSHIK

July 2017

Was the Jury Wrong About Toyota's Software?

How questionable testimony on embedded software tipped the scales.

April 2018

SSIT Awards and Recognition

2018 IEEE SSIT Carl Barus Award Announced

Submitted by Bradley Kjell, SSIT Awards Chair

The IEEE Society on Social Implications of Technology is pleased to announce that Dr. Philip Koopman has been awarded the 2018 IEEE-SSIT Carl Barus Award for Outstanding Service in the Public Interest. The citation of the award reads: "For uncovering major automotive software defects causing unintended acceleration, and despite attacks, publicizing and successfully testifying about its dangers."

Dr. Koopman is an associate professor of Electrical and Computer Engineering at Carnegie Mellon University. His research interests include self-driving car safety, dependable embedded systems, and embedded systems security. His investigations into automotive throttle control computer systems revealed safety-critical design defects. This work should inform not only future designers of safety-critical software for automobiles but also all computer-based system designers.

The Barus Award is bestowed to an individual or group who has acted within the field of interest of the IEEE to protect the health, safety or welfare of the public, despite risk to their career and professional reputation. More information about the award is on our website.

The award will be presented during SSIT's annual conference, ISTAS, which takes place 13-14 November 2018 in Washington, DC, USA. Dr. Koopman will be one of the speakers at the conference.

Conclusions

Carnegie Mellon University

- Suggest you ***follow the links*** from the paper

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