Automotive Safety Practices vs. Accepted Principles

SAFECOMP, Sept. 2018

Prof. Philip Koopman
Overview

■ “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
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-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

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.


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

https://www.wired.com/2010/03/unintended-acceleration/
Gas/Brake confusion about 0.1% of crashes (Pre-ETC data)

- 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

Camry UA VOQ Rate by Model Year

NHTSA slide from 2010 / Owner UA complaint rates

http://onlinepubs.trb.org/onlinepubs/ua/100630DOTSlides.pdf
© 2018 Philip Koopman
US Government Position on Toyota UA

- **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**

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

---

**Toyota "Unintended Acceleration" Has Killed 89**

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.


© 2018 Philip Koopman
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

- 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: PknOqXqcnI0, M1XHjl_6htM, 0hE6gaCbyg, y6Knn4TazMg
Current US Regulatory Strategy

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

- 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

- **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

[Link to article](https://goo.gl/RQi1ik)
[Link to image](https://goo.gl/PRLKNS)
And Now: Self Driving Cars

- **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.
A Cautionary Tale for Academics

Embedded Software Under the Courtroom Microscope

A Case Study of the Toyota Unintended Acceleration Trial

December 2016

Was the Jury Wrong About Toyota’s Software?

How questionable testimony on embedded software tipped the scales.

July 2017

SSIT Awards and Recognition

2018 IEEE SSIT Carl Barus Award Announced

Submitted by Bradley Kel, 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.

April 2018

© 2018 Philip Koopman
Conclusions

Suggest you *follow the links* from the paper

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

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