EE Live!

#KillerApps

KILLER APPS
Embedded Software's Greatest Hit Jobs

April 1, 2014

Michael Barr

@embeddedbarr

BARR group

The Embedded Systems Experts

#KillerApps

MICHAEL BARR
Co-Founder/CTO, Barr Group

Electrical Engineer (BSEE/MSEE)

Experienced Embedded Software Developer

Consultant & Trainer (1999-present)

- Embedded software process and architecture improvement
- Various industries (e.g., medical devices, industrial controls)

Former *Adjunct Professor*

- University of Maryland 2000-2003 (Design and Use of Operating Systems)
- Johns Hopkins University 2012 (Embedded Software Architecture)

Served as *Editor-in-Chief*, *Columnist*, *Conference Chair*

Expert witness (software patents/copyrights, product liability)

Author of 3 books and 70+ articles/papers

BARR group

#KillerApps

BARR GROUP
The Embedded Systems Experts

Skills Training

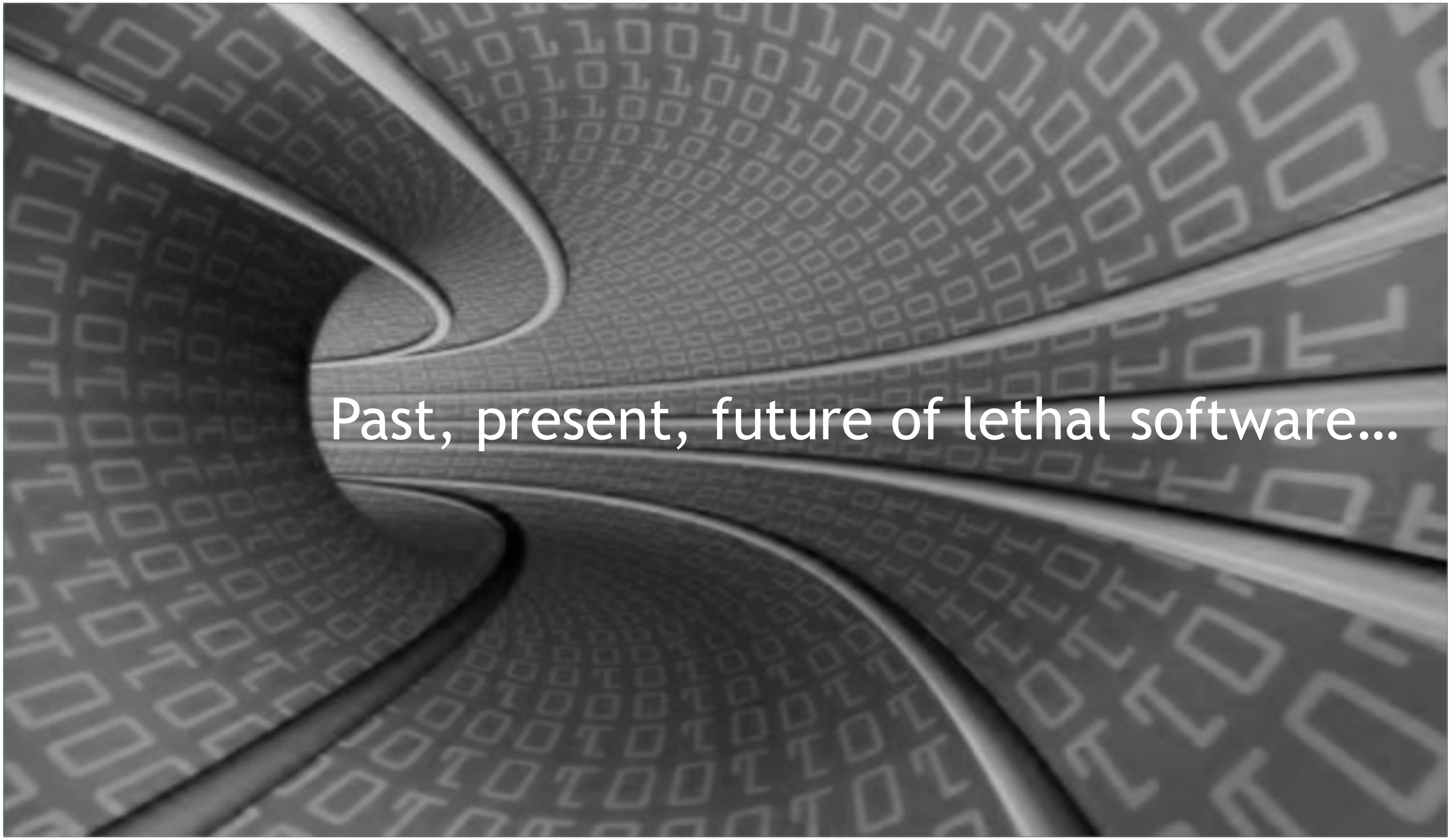
In this age of quickly changing technology everyone needs training from time to time. We provide skills training online and on-site to keep you up to date with the latest in embedded systems technology.

Barr Group helps companies make their embedded systems safer and more secure.

@barrgroup #embedsys #safety #security

#KillerApps

SAFETY & EMBEDDED SOFTWARE



Past, present, future of lethal software…

SAFETY PAST

Patriot Missile

- Failed to track a Scud

Therac-25

- Massive overradiation

Combined cost

- 30 dead
- >100 injured

"Today's Grim Reaper doesn't bother with a scythe."

http://jasonlove.com/funny-cartoons/search-viewer.aspx?id=1125

PATRIOT MISSILE FAILURE

GAO: Software Problem Led to System Failure at Dhahran, Saudi Arabia

February 25, 1991

- 28 U.S. soldiers dead; 98 wounded
- Single deadliest incident for U.S.

#KillerApps

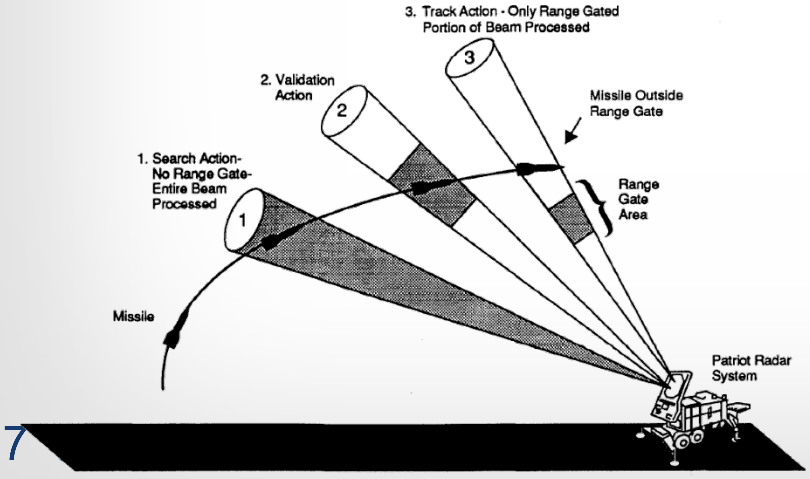
THE PATRIOT SOFTWARE BUG

Two versions of system time

- Timer chip integer representation
- Software fixed-point binary format

7.5s: $000000000000000000000111.100000000000000000000000_2$

Increasing inaccuracy…


3. Track Action - Only Range Gated Portion of Beam Processed
3
2. Validation Action
2
Missile Outside Range Gate
1. Search Action- No Range Gate- Entire Beam Processed
1
Range Gate Area
Missile
Patriot Radar System

uptime (h)	error (s)	shift (m)
1	.0034	7
8	.0275	55
20	.0687	137
100	.3433	687

BARR group

GAO Report: https://www.fas.org/spp/starwars/gao/im92026.htm

#KillerApps

NOTEWORTHY QUOTES

Brig. Gen. Neal, U.S. Command (+2 *days*)

- "looks like this [Scud] broke apart in flight … [thus] **wasn't in the parameters where it could be attacked**"

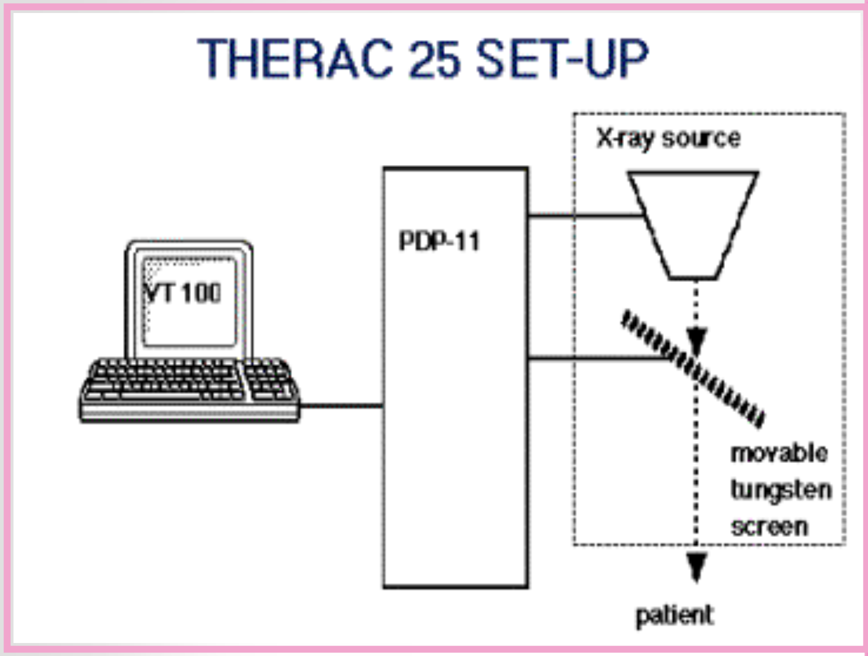
Col. Garnett, Patriot Program Director (+4 *months*)

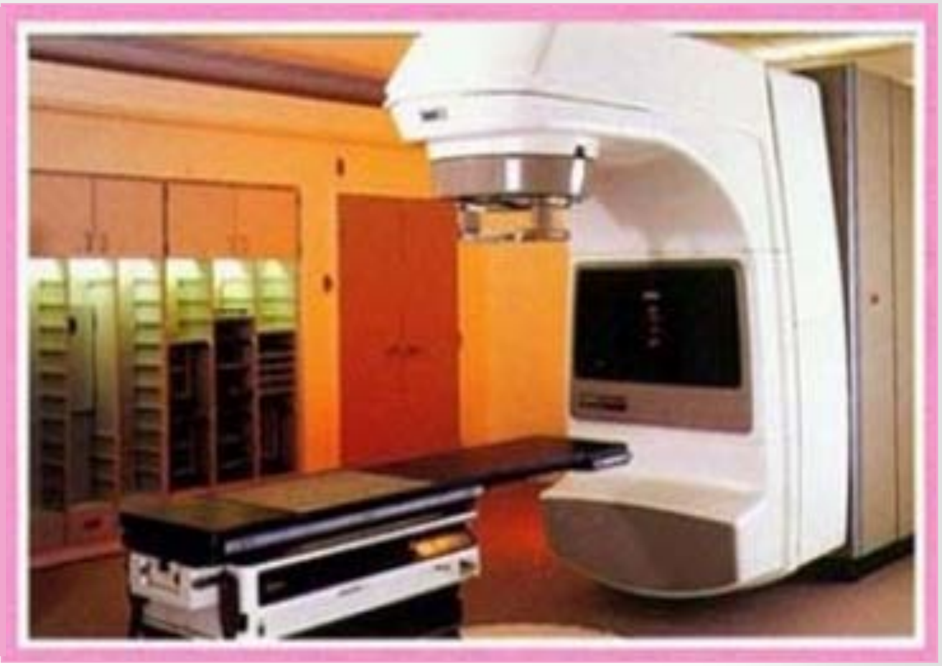
- "an anomaly that **never showed up in thousands of hours of testing**"

Sources: Contemporaneous *New York Times* articles; available online.

#KillerApps

THERAC-25 SYSTEM OVERVIEW





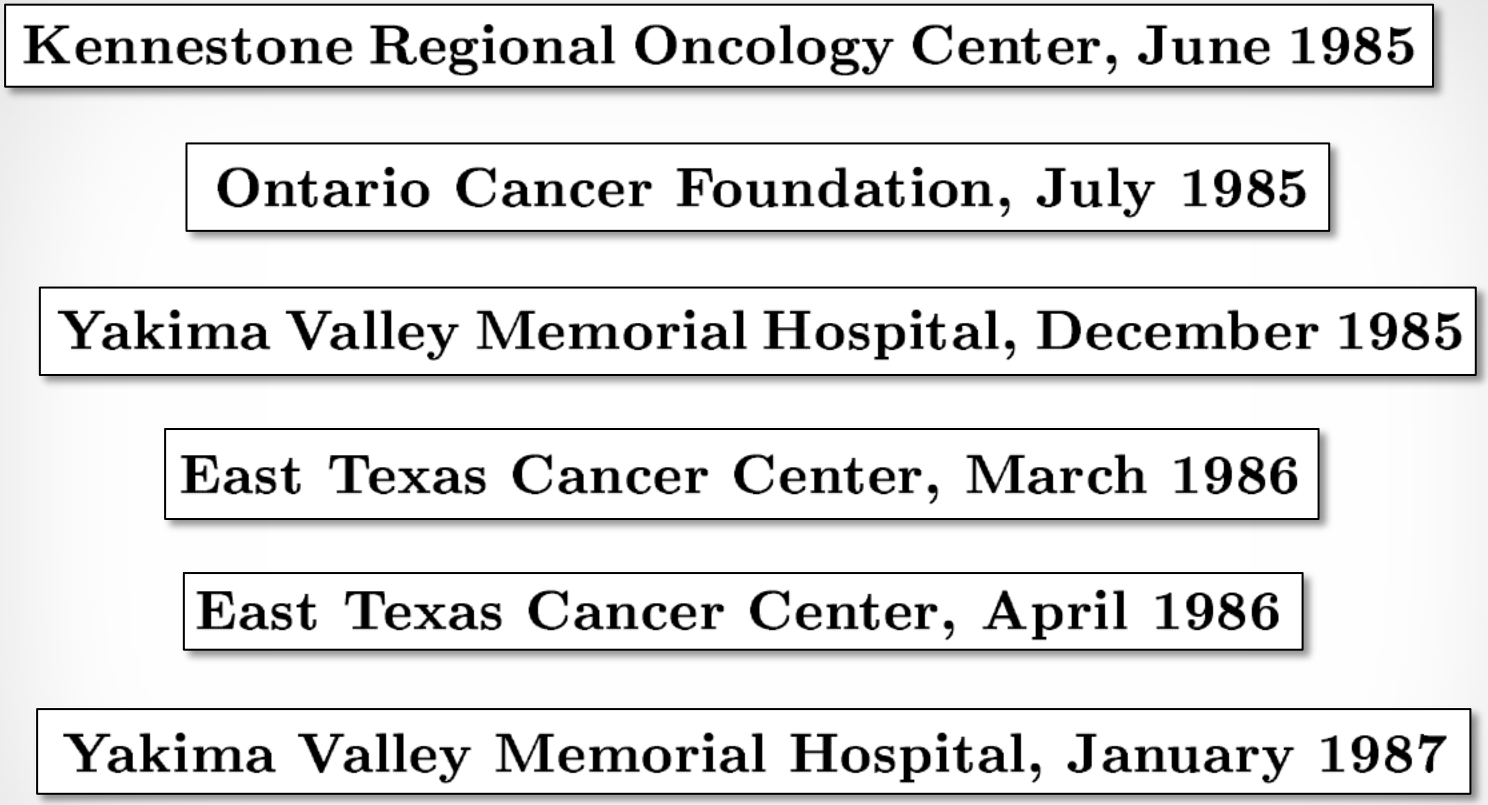
Installations in 5 U.S. and 6 Canadian facilities

- Thousands of treatments as intended, but…

Images: http://hci.cs.siue.edu/NSF/Files/Semester/Week13-2/PPT-Text/Slide13.html

#KillerApps

6 MASSIVE OVER-DOSES



Kennestone Regional Oncology Center, June 1985

Ontario Cancer Foundation, July 1985

Yakima Valley Memorial Hospital, December 1985

East Texas Cancer Center, March 1986

East Texas Cancer Center, April 1986

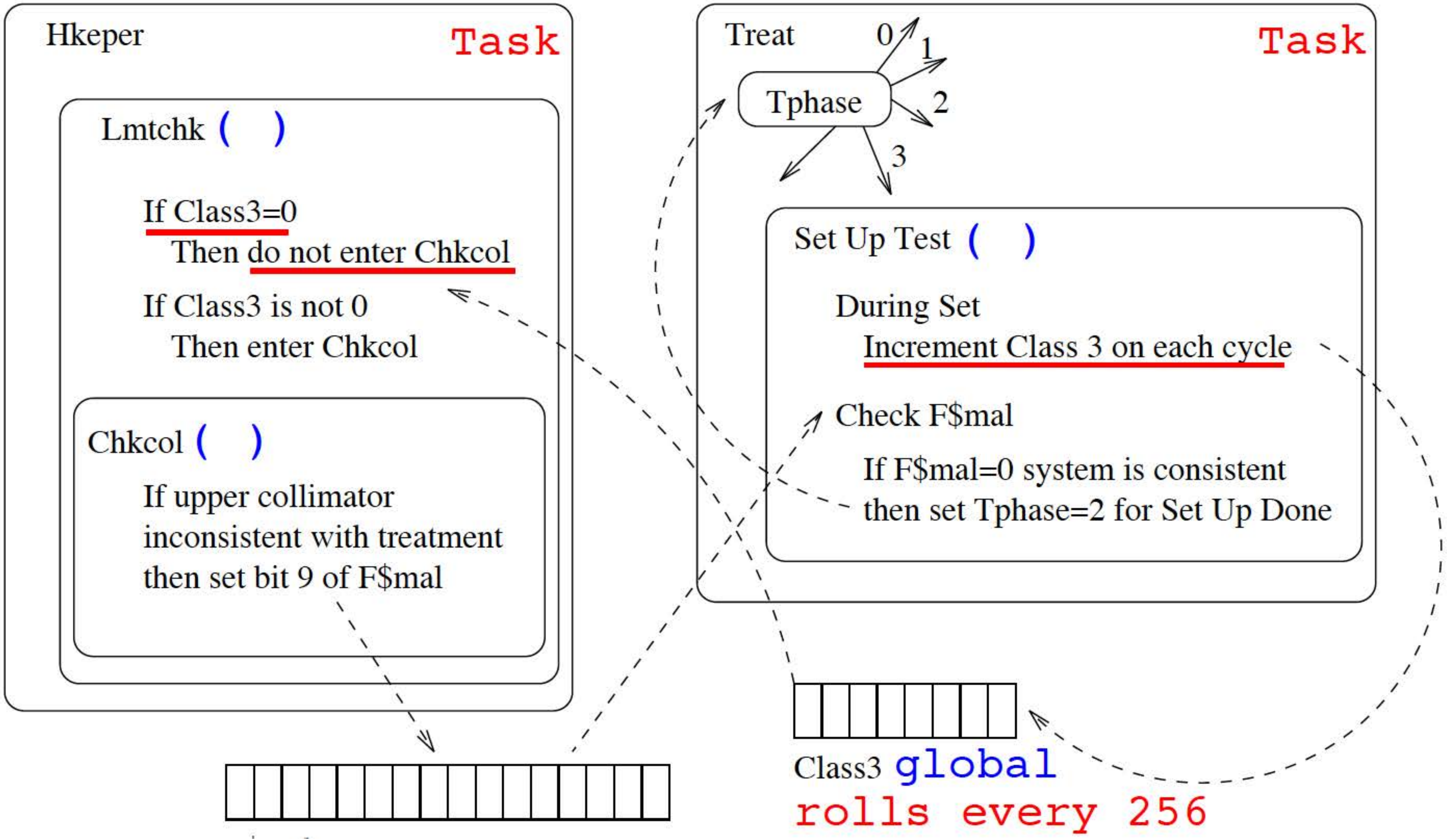
Yakima Valley Memorial Hospital, January 1987

BARR group

Source: http://sunnyday.mit.edu/papers/therac.pdf

#KillerApps

ONE OF THE THERAC-25 BUGS



Hkeper

Task

Lmtchk ( )

If Class3=0
Then do not enter Chkcol

If Class3 is not 0
Then enter Chkcol

Chkcol ( )

If upper collimator inconsistent with treatment then set bit 9 of F$mal

Treat

Task

Tphase

Set Up Test ( )

During Set
Increment Class 3 on each cycle

Check F$mal

If F$mal=0 system is consistent
then set Tphase=2 for Set Up Done

Class3 global
rolls every 256

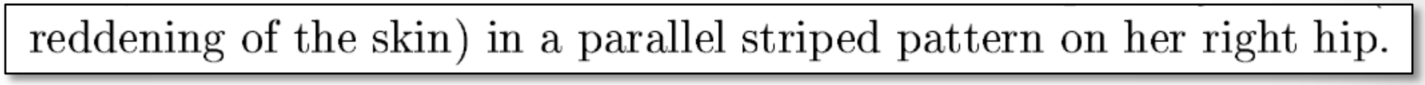
Source: http://sunnyday.mit.edu/papers/therac.pdf

NOTEWORTHY QUOTES

AECL Letter (*Feb ’86, in response to 3rd incident*)

- “After careful consideration we are of the opinion that **this [injury] could not have been produced by any malfunction** of the Therac-25”

“no other instances of similar [patient] damage”



reddening of the skin) in a parallel striped pattern on her right hip.

Quality Assurance Manager (*to User’s Group*)

- Therac-25 software was tested for “2,700 hours”

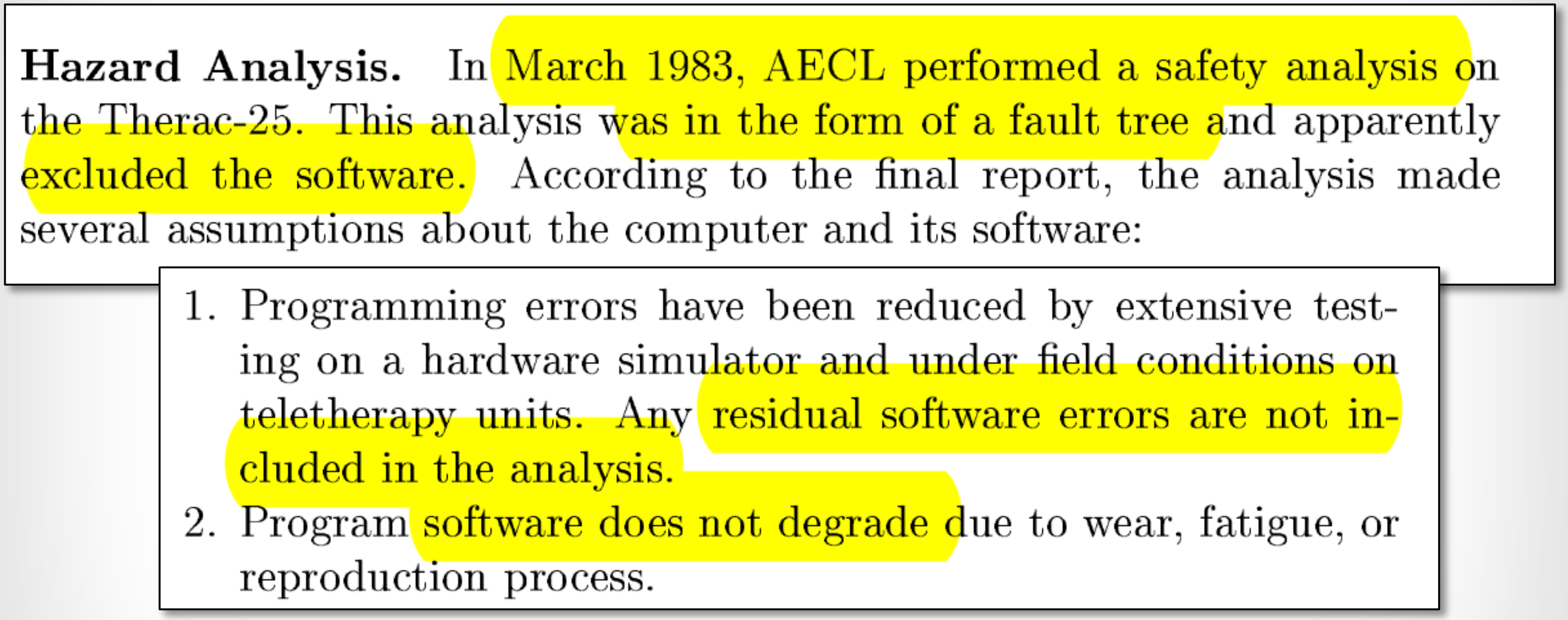
Under questioning: “2,700 hours of use”

Source: http://sunnyday.mit.edu/papers/therac.pdf

#KillerApps

THERAC-25 LESSONS LEARNED

Underestimation of software risks can be deadly



Hazard Analysis. In March 1983, AECL performed a safety analysis on the Therac-25. This analysis was in the form of a fault tree and apparently excluded the software. According to the final report, the analysis made several assumptions about the computer and its software:

1. Programming errors have been reduced by extensive testing on a hardware simulator and under field conditions on teletherapy units. Any residual software errors are not included in the analysis.
2. Program software does not degrade due to wear, fatigue, or reproduction process.

More: Leveson, *IEEE Computer*, Jul 1993

Source: http://sunnyday.mit.edu/papers/therac.pdf

SAFETY PRESENT

Some systems are "safety-critical"

Exposure to low probability events…

- Random events in the electronics,
- Bugs latent in the software, and/or
- Unforeseen gaps through fail-safes

Testing cannot prove absence of bugs/gaps…

- Therefore, system safety only as by design

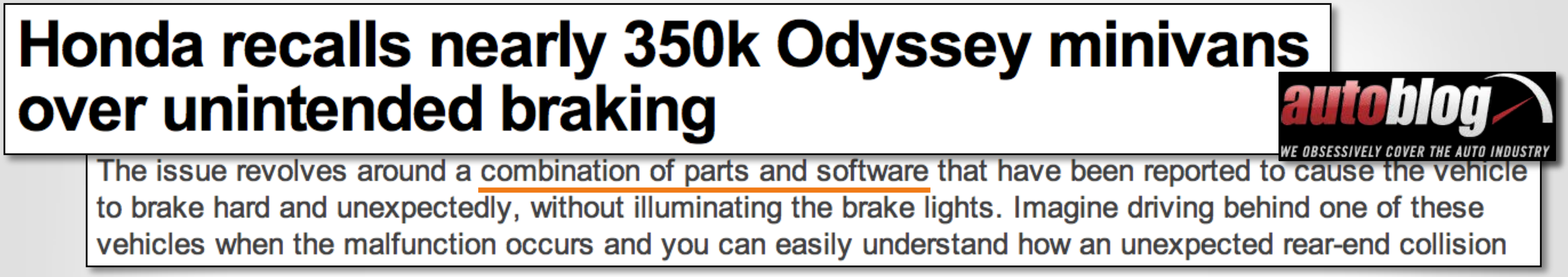
#KillerApps

AUTOMOTIVE SOFTWARE TRENDS

Image: http://gearheads.org/understanding-the-brain-at-the-heart-of-your-car/

AUTOMOTIVE SOFTWARE RECALLS

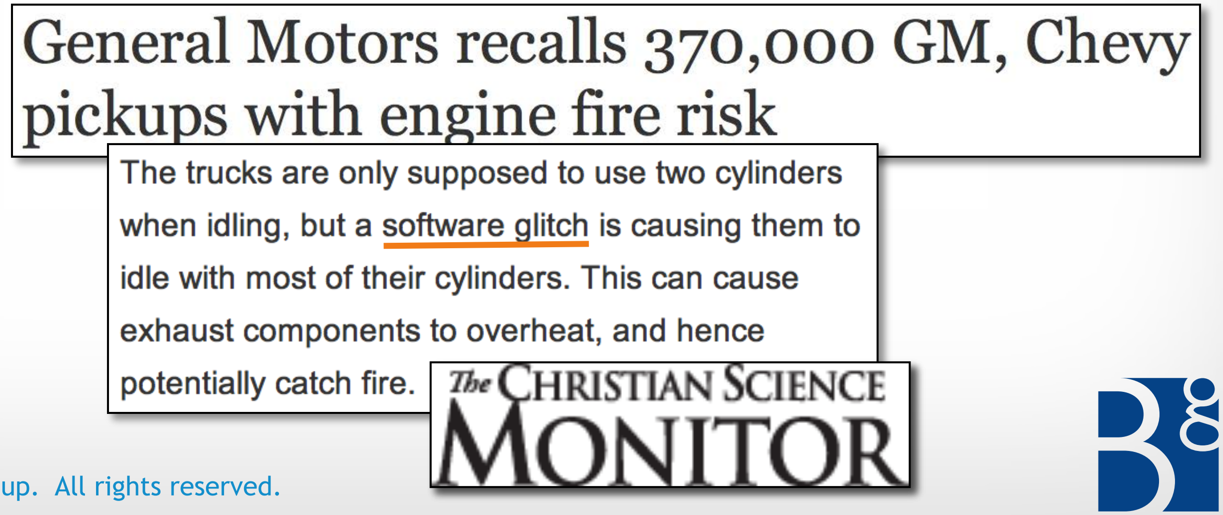
RECALLS



Honda recalls nearly 350k Odyssey minivans over unintended braking

autoblog WE OBSESSIVELY COVER THE AUTO INDUSTRY

The issue revolves around a combination of parts and software that have been reported to cause the vehicle to brake hard and unexpectedly, without illuminating the brake lights. Imagine driving behind one of these vehicles when the malfunction occurs and you can easily understand how an unexpected rear-end collision



General Motors recalls 370,000 GM, Chevy pickups with engine fire risk

The trucks are only supposed to use two cylinders when idling, but a software glitch is causing them to idle with most of their cylinders. This can cause exhaust components to overheat, and hence potentially catch fire.

The Christian Science Monitor

TOYOTA & UNINTENDED ACCELERATION

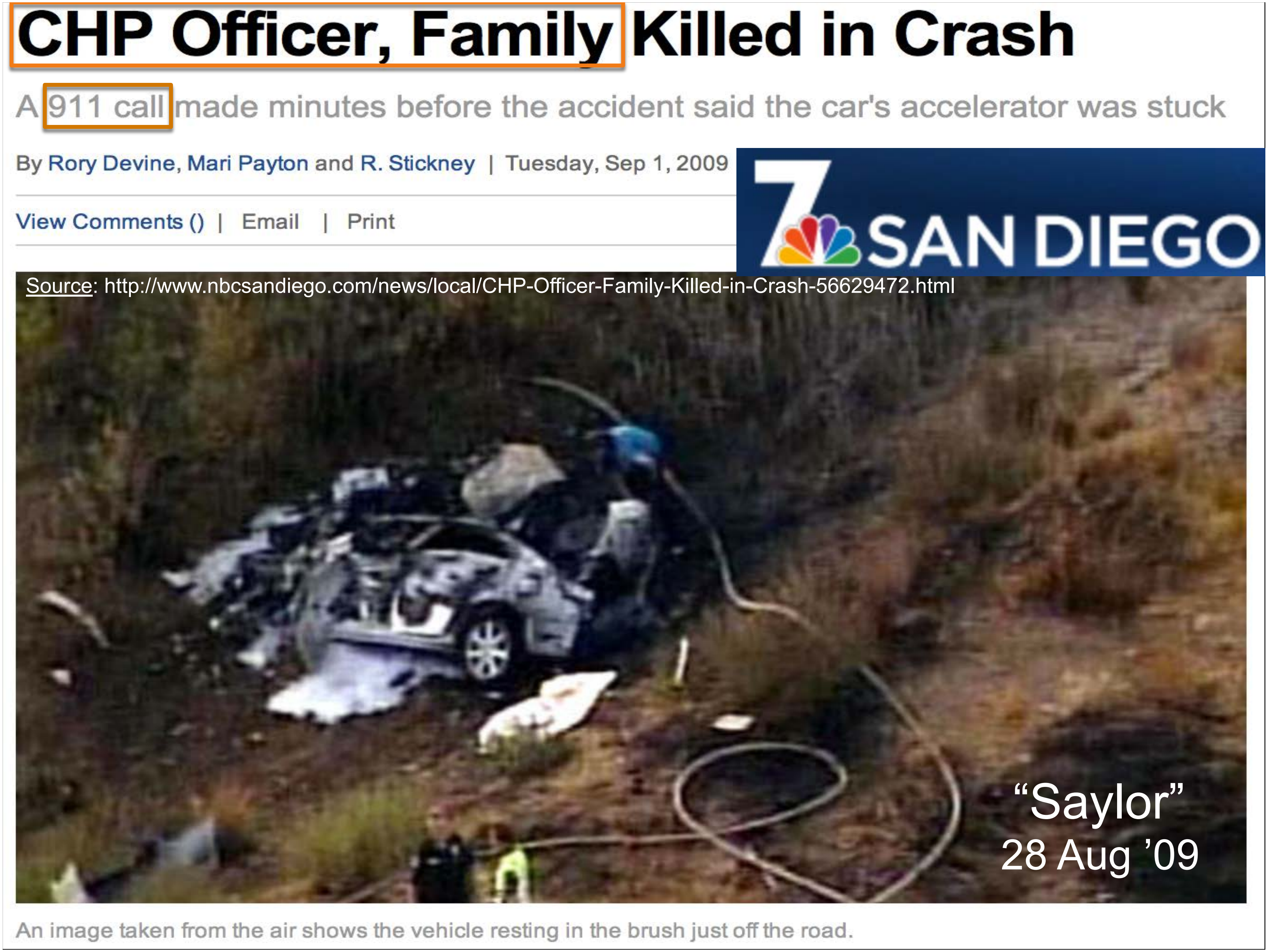
Toyota adds “electronic throttle” ~2002 models

NHTSA investigates “UA” complaints (5 times)

Models at Issue	End Date	Recall?
2002-2005 Camry/Solara, Lexus ES	Jan ‘06	none
2002-2006 Camry/Solara	Apr ‘07	none
2007-2008 Camry, Lexus ES	Sep ‘07	all-weather floor mat
2006-2007 Tacoma	Aug ‘08	none
2004 Sienna	Jan ‘09	trim clip

Then a high profile crash…

Timeline: https://www.consumerreports.org/cro/news/2010/02/timeline-of-toyota-acceleration-investigations/index.htm



CHP Officer, Family Killed in Crash

A 911 call made minutes before the accident said the car's accelerator was stuck

By Rory Devine, Mari Payton and R. Stickney | Tuesday, Sep 1, 2009

View Comments () | Email | Print

Source: http://www.nbcsandiego.com/news/local/CHP-Officer-Family-Killed-in-Crash-56629472.html

“Saylor”
28 Aug ’09

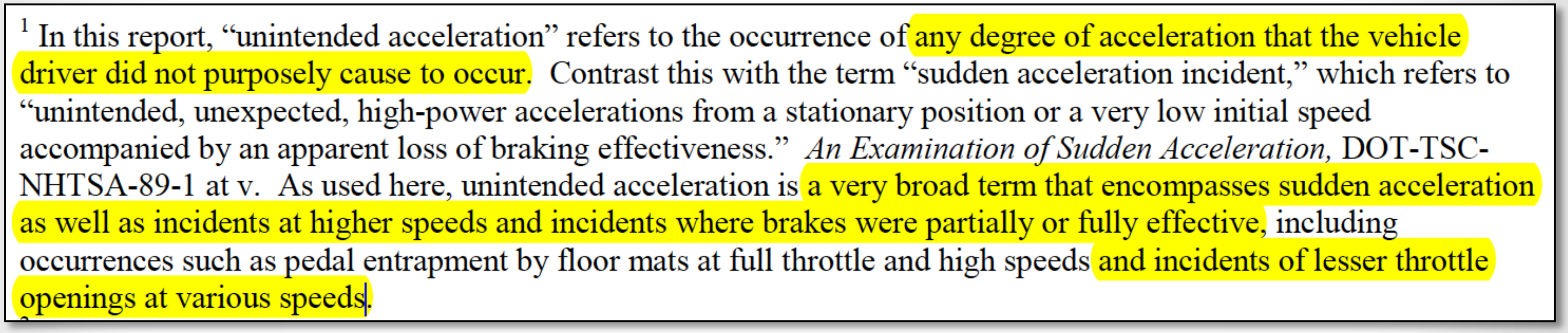
An image taken from the air shows the vehicle resting in the brush just off the road.

#KillerApps

UNINTENDED ACCELERATION

What is unintended acceleration?

- Acceleration the driver did not purposely cause



[1] In this report, "unintended acceleration" refers to the occurrence of any degree of acceleration that the vehicle driver did not purposely cause to occur. Contrast this with the term "sudden acceleration incident," which refers to "unintended, unexpected, high-power accelerations from a stationary position or a very low initial speed accompanied by an apparent loss of braking effectiveness." *An Examination of Sudden Acceleration,* DOT-TSC-NHTSA-89-1 at v. As used here, unintended acceleration is a very broad term that encompasses sudden acceleration as well as incidents at higher speeds and incidents where brakes were partially or fully effective, including occurrences such as pedal entrapment by floor mats at full throttle and high speeds and incidents of lesser throttle openings at various speeds.

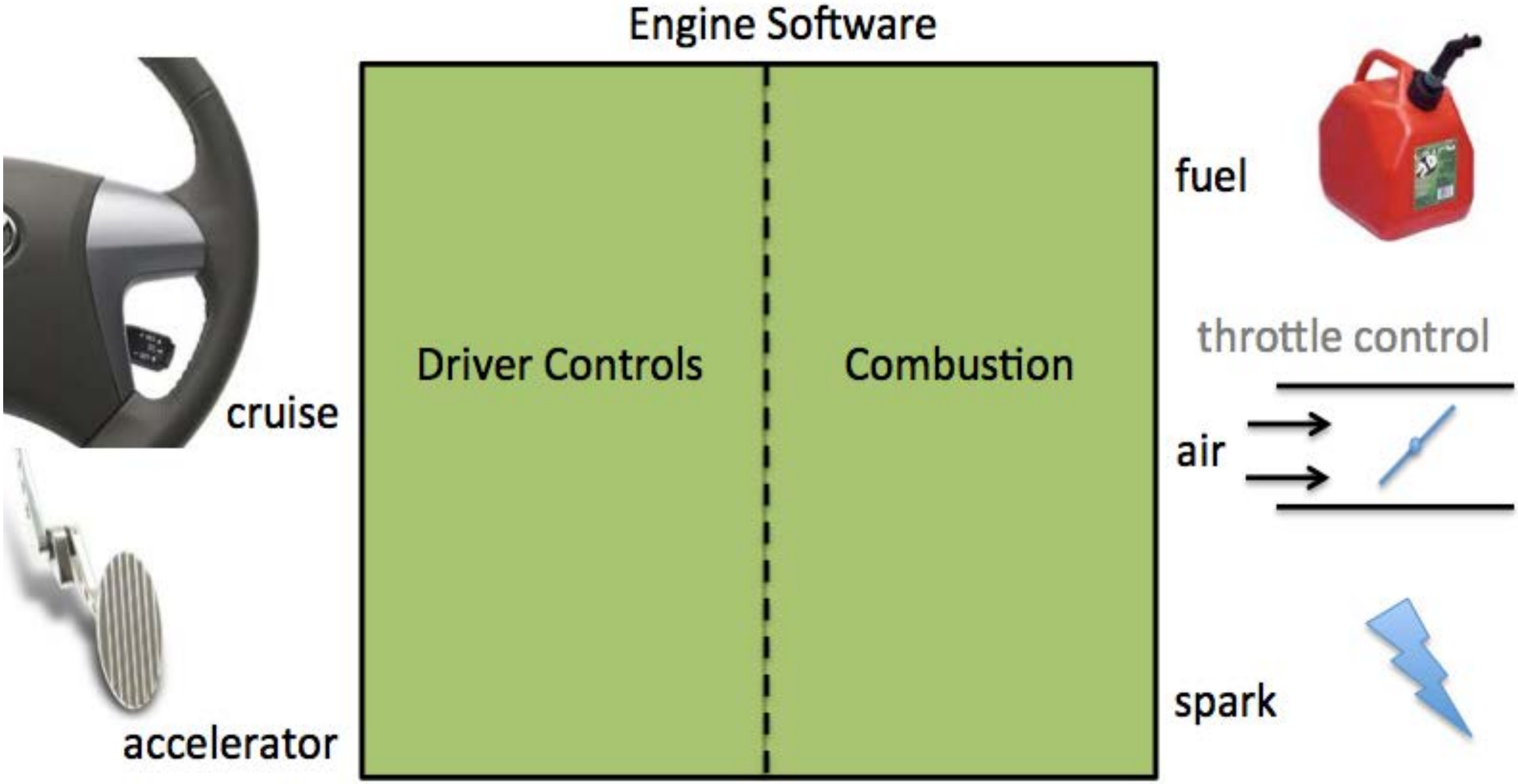
Loss of driver control of engine power

- A very dangerous vehicle malfunction!

BARR group

Source: http://www.nhtsa.gov/staticfiles/nvs/pdf/NHTSA-UA_report.pdf ("NHTSA"), p. vi

ELECTRONIC THROTTLE CONTROL



Engine Software

cruise

accelerator

Driver Controls

Combustion

fuel

throttle control

air

spark

#KillerApps

POSSIBLE SOURCES OF ACCELERATION

Mechanical

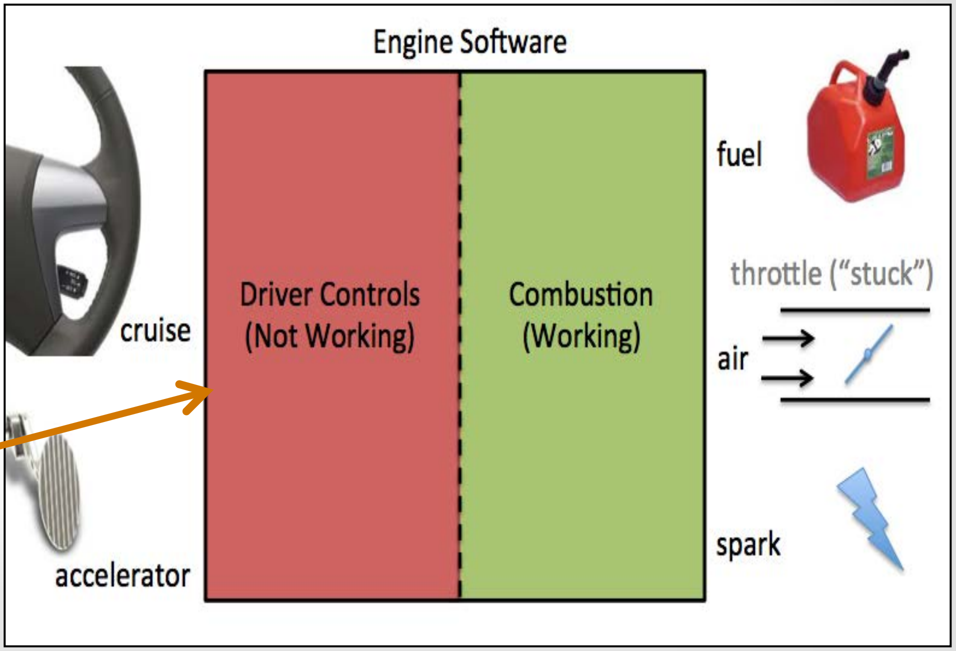
- Pedal entrapped by floor mat
- Sticky pedal by internal defect
- Stuck throttle valve

~30% of models recalled

Driver error

- "Pedal misapplication"

Software malfunction



TOYOTA'S HIGH COMPLAINT RATE

Complaints jump after "electronic throttle"

- NHTSA data 2004 vs. 2000-2003

All UA complaints ~2,000 (vs. 1,200-1,400)

Toyota's percentage ~20% (vs. 4-7%)

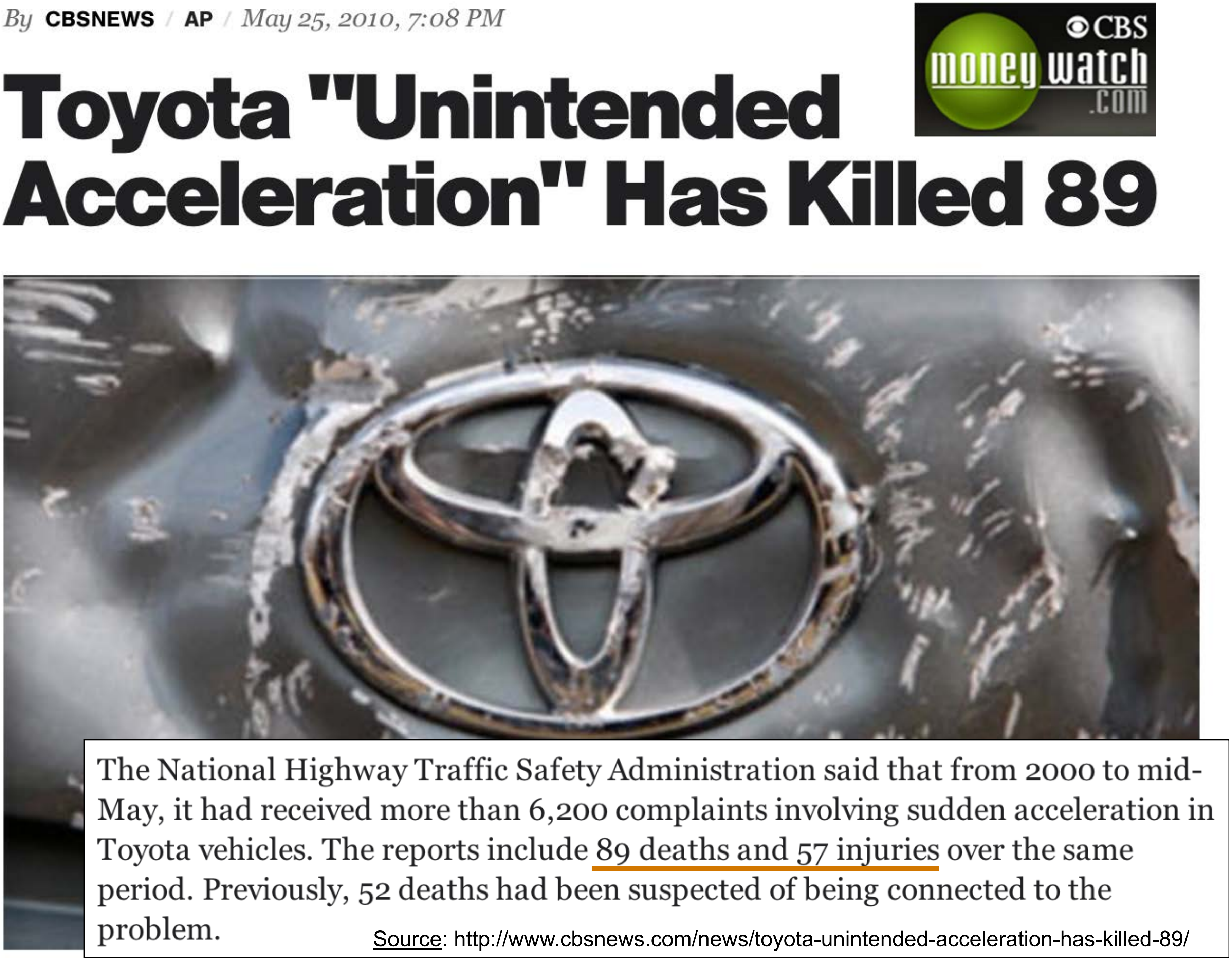
Toyota +300%

<u>Complaint Statistics</u>: http://democrats.energycommerce.house.gov/Press_111/20100222/ Detailed.Timeline.and.Background.of.NHTSA.Actions.Regarding.Toyota.Sudden.Acceleration.pdf

Could driver errors explain the jump?

- Expect driver errors ~even across makes
- Why such a big increase w/in Toyota?

BARR group



By **CBSNEWS** / **AP** / *May 25, 2010, 7:08 PM*

Toyota "Unintended Acceleration" Has Killed 89

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.

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

Statistical analysis and slide by R.A. Whitfield to NAS' Transportation Research Board (Oct 2010)

How likely is it that these factors...

Vehicle Factors:
Floor mats
Sticky pedals
Pedal placement
Gated gear shift pattern
Ignition switch design

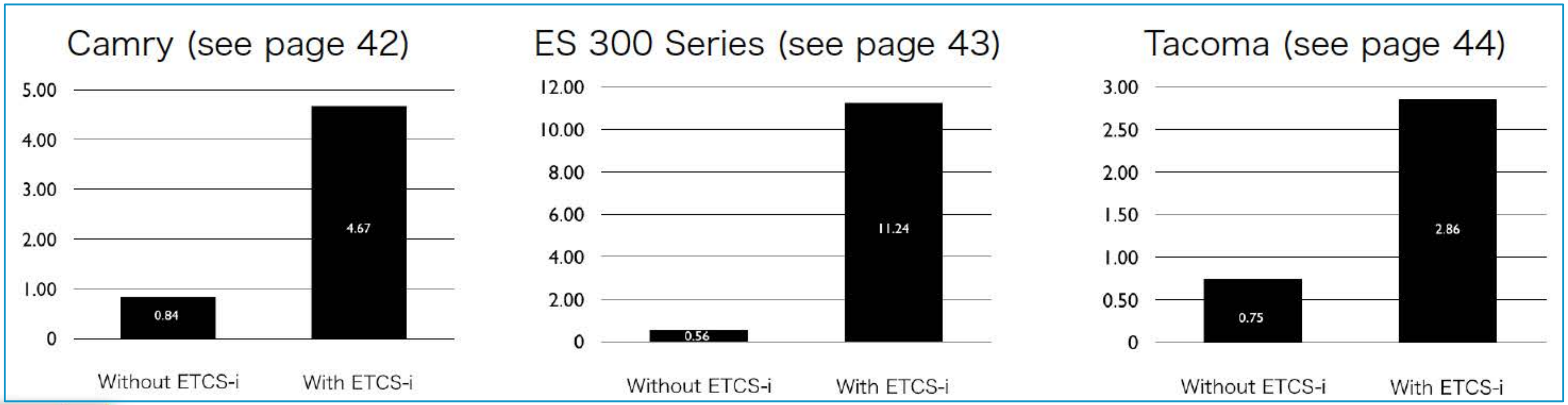
Recalls of some cars.

Driver Factors:
Mass hysteria
Fraud
Old age
Youth
Inexperience
Incompetent drivers

Factors held ~constant.

Environmental/Usage Factors

...explain these results when controlling for make/model and years in service?



UA complaints to NHTSA "pre-Saylor", in 1st year of model sale per 100K.

Source: http://onlinepubs.trb.org/onlinepubs/UA/101011Whitfield.pdf

"THE NASA REPORT"

At NHTSA's request

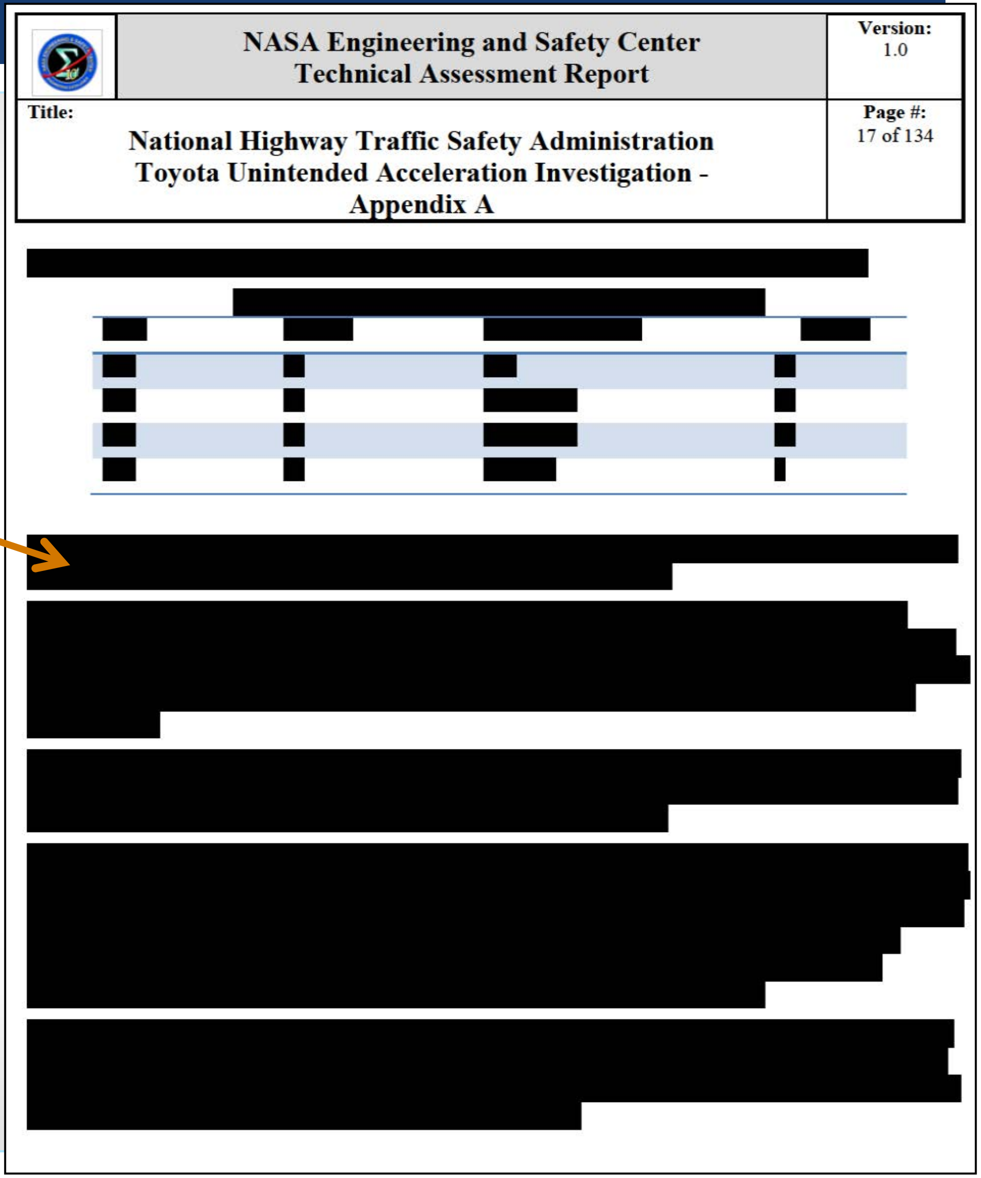
- Published Feb '11

Lots of redactions

- Especially re: software
- *I can't talk about them!*

Some flaws found…

…but not "the cause"



NASA Engineering and Safety Center Technical Assessment Report	Version: 1.0
Title: National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation - Appendix A	Page #: 17 of 134

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

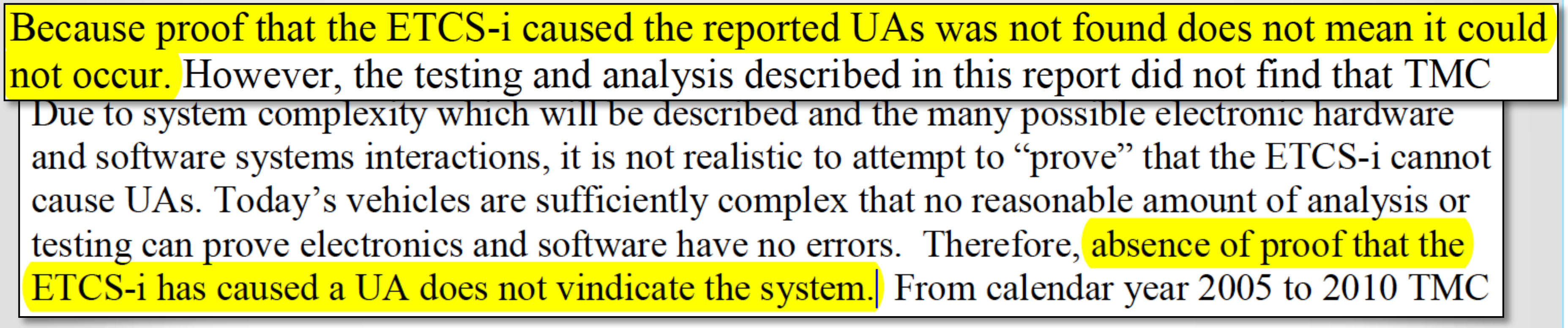
[redacted]

[redacted]

Public (Redacted) NASA Report: https://www.nhtsa.gov/UA

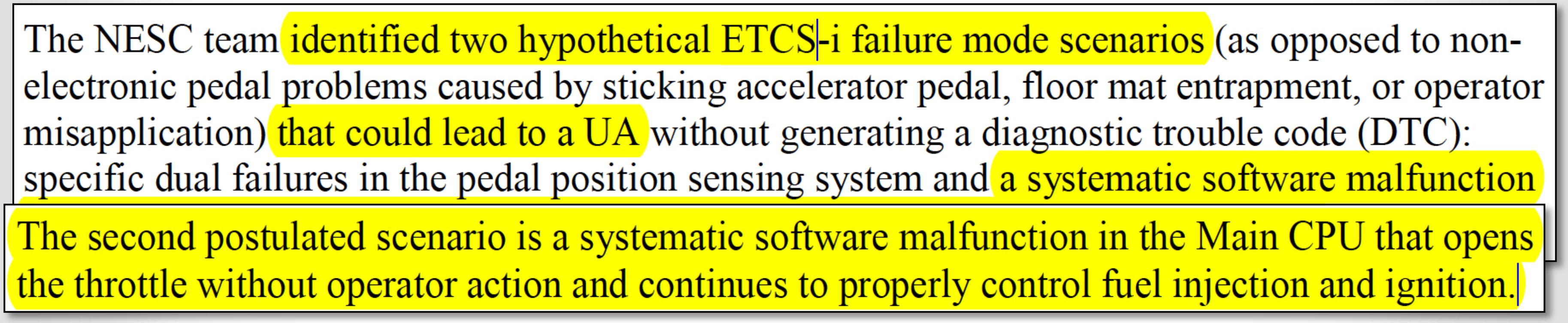
#KillerApps

KEY NASA STATEMENTS



Because proof that the ETCS-i caused the reported UAs was not found does not mean it could not occur. However, the testing and analysis described in this report did not find that TMC

Due to system complexity which will be described and the many possible electronic hardware and software systems interactions, it is not realistic to attempt to "prove" that the ETCS-i cannot cause UAs. Today's vehicles are sufficiently complex that no reasonable amount of analysis or testing can prove electronics and software have no errors. Therefore, absence of proof that the ETCS-i has caused a UA does not vindicate the system. From calendar year 2005 to 2010 TMC



The NESC team identified two hypothetical ETCS-i failure mode scenarios (as opposed to non-electronic pedal problems caused by sticking accelerator pedal, floor mat entrapment, or operator misapplication) that could lead to a UA without generating a diagnostic trouble code (DTC): specific dual failures in the pedal position sensing system and a systematic software malfunction

The second postulated scenario is a systematic software malfunction in the Main CPU that opens the throttle without operator action and continues to properly control fuel injection and ignition.

BARR group

Source: http://www.nhtsa.gov/staticfiles/nvs/pdf/NASA-UA_report.pdf ("NASA"), pp. 15-20

#KillerApps

LAWSUITS…

Toyota had to produce source code and design docs

- Lawyers for lead U.S. plaintiffs brought in Barr Group

Plaintiff	Court	My Role	Status	Amount
Saylor	CA	*	settled Feb ‘11	$10M
Van Alfen	U.S.	report Jul ’12	settled Dec ’12	private
U.S. Class	U.S.	report Jul ’12	settled Dec ’12	up to $1.5B
St. John	U.S.	report Apr ’13	in talks now	
Bookout	OK	testimony Oct ’13	jury trial Oct ‘13	

* Saylor (and some other early plaintiffs) did not look into software.

BARR group

#KillerApps

OUR REVIEW OF TOYOTA'S SOFTWARE

Access to Toyota's engine source code

- Seven Toyota and Lexus models x ~2002-2010 model yrs

Approximately 18 months of calendar time

- By an experienced team of embedded practitioners
- Building on NASA's earlier work; digging deeper
    - *Access to more software/code (per vehicle)*
    - *Bottom-up focus on software details*
    - *Simulation and in-vehicle testing*

#KillerApps

SOURCE CODE CONFIDENTIALITY

Custom-built room

- No Internet
- No phones

Layered security

- Guard station
- More… *I can't say!*

At a secret address…

BARR group

Photo: Not of the actual source code room.

BOOKOUT FACTS

Single-vehicle Sep 2007 accident

- On exit ramp from US-69 South

  Near Eufaula Lake, Oklahoma

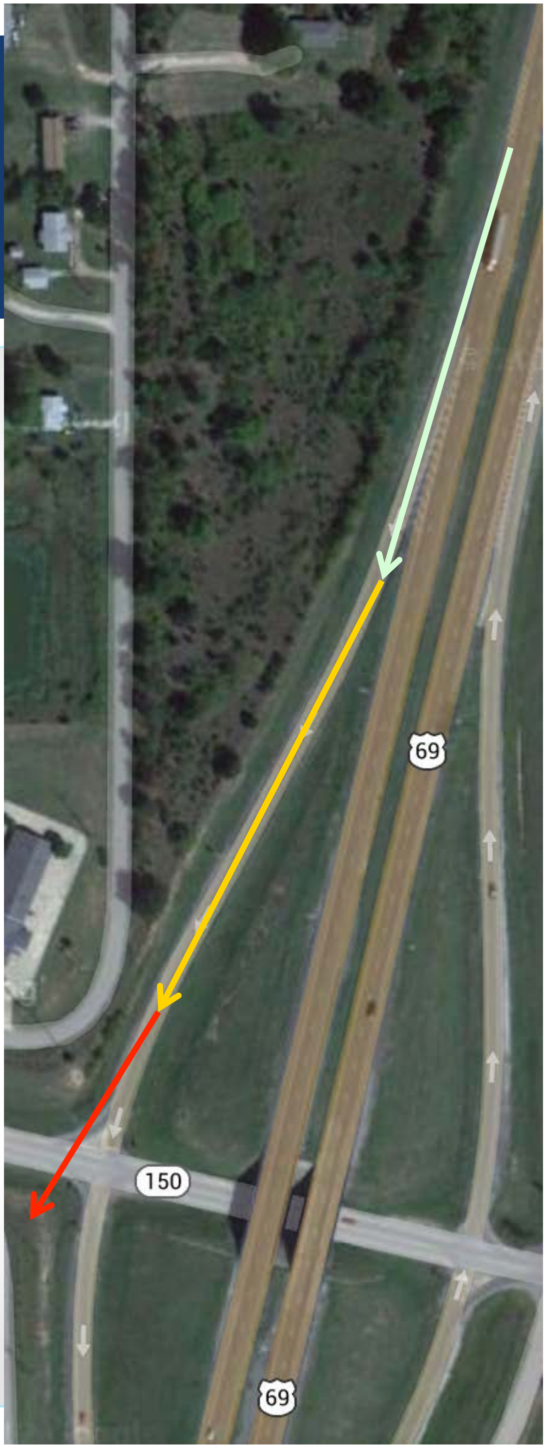
Vehicle

- 2005 Toyota Camry (4-cylinder)

Two occupants

- Driver Jean Bookout: *seriously injured*
- Passenger Barbara Schwarz: *died later*

  Witness to driver's braking



#KillerApps

BOOKOUT RECONSTRUCTION

Speed estimates

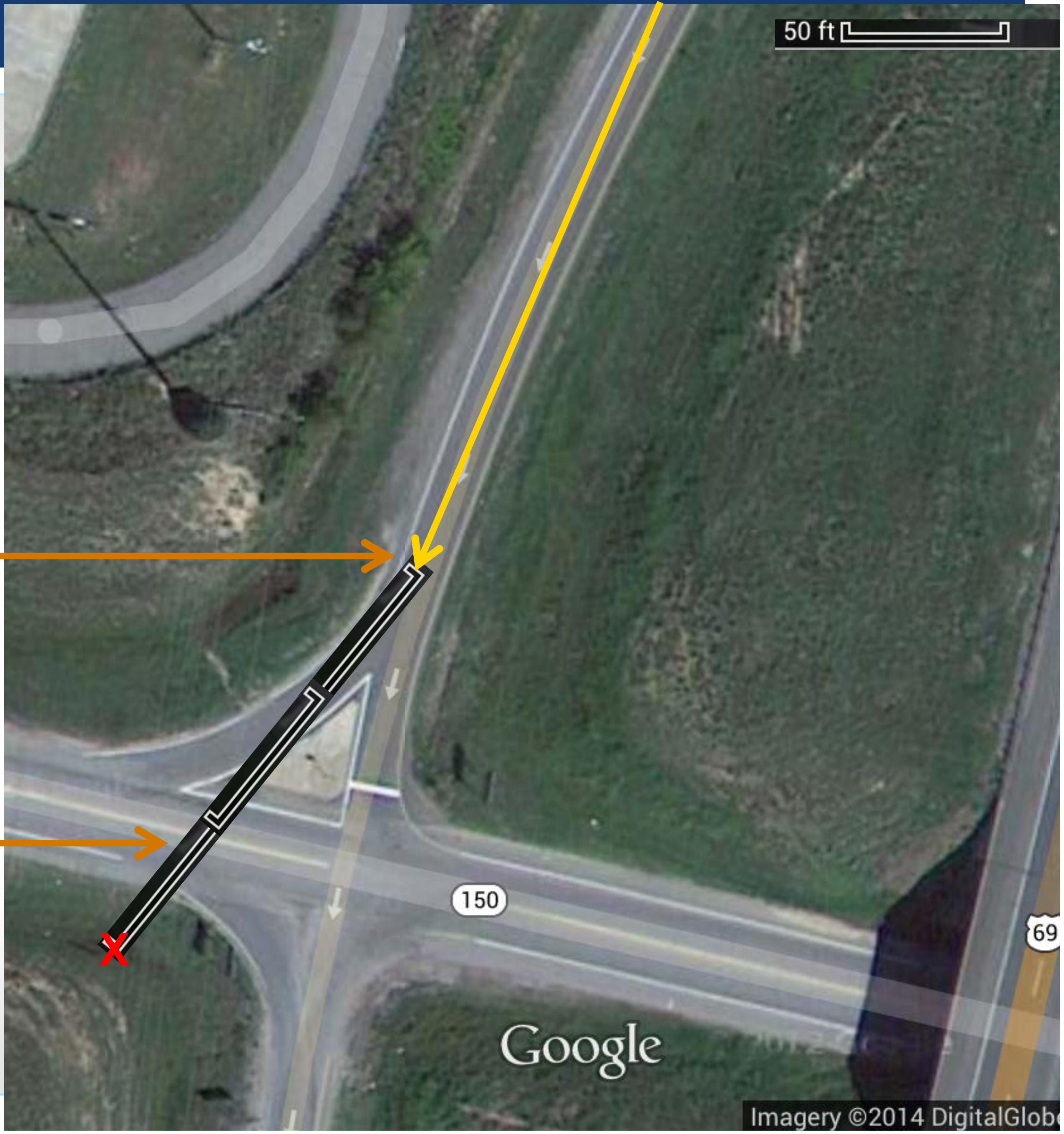
- Skid start ~50mph
- At impact ~25mph

Agreed she braked

- Parking brake too?

150’ skid mark

- Way too long!



#KillerApps

OPEN THROTTLE DEGRADES BRAKING

Proof via Saylor crash

- "Pedal stuck"

  Top speed ~120 mph
- Healthy male age 45

  Couldn't stop by braking

Consumer Reports

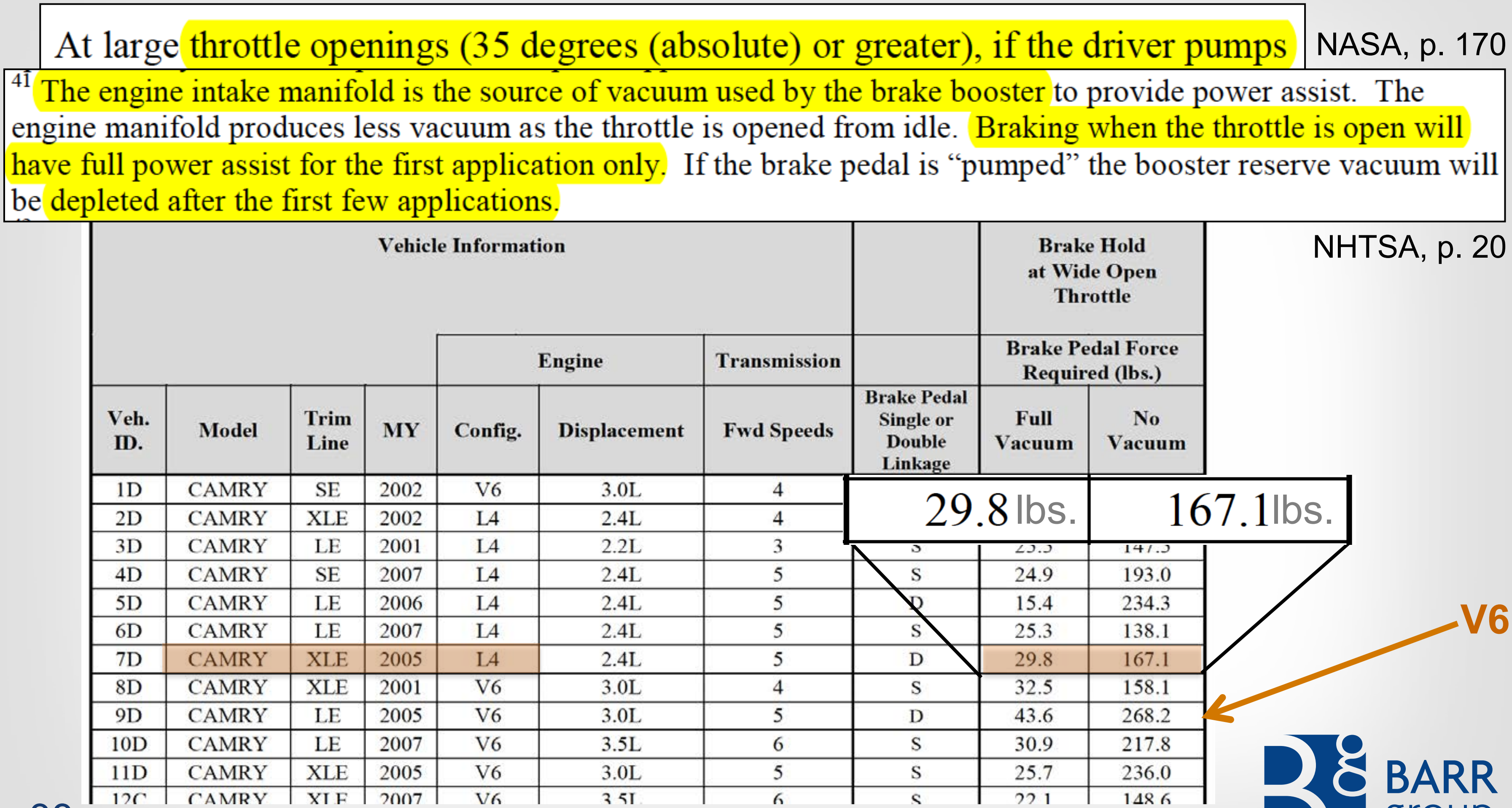
- *"80 miles an hour. I am powerless to slow this vehicle"*
- After pumping… "*even one time … it becomes almost impossible to stop the vehicle.*"

BARR group

Consumer Reports Video: http://youtu.be/VZZNR9O3xZM

#KillerApps

BRAKE VS. THROTTLE DATA POINTS



At large throttle openings (35 degrees (absolute) or greater), if the driver pumps

NASA, p. 170

[41] The engine intake manifold is the source of vacuum used by the brake booster to provide power assist. The engine manifold produces less vacuum as the throttle is opened from idle. Braking when the throttle is open will have full power assist for the first application only. If the brake pedal is "pumped" the booster reserve vacuum will be depleted after the first few applications.

NHTSA, p. 20

Vehicle Information								Brake Hold at Wide Open Throttle	
				Engine		Transmission		Brake Pedal Force Required (lbs.)	
Veh. ID.	Model	Trim Line	MY	Config.	Displacement	Fwd Speeds	Brake Pedal Single or Double Linkage	Full Vacuum	No Vacuum
1D	CAMRY	SE	2002	V6	3.0L	4			
2D	CAMRY	XLE	2002	L4	2.4L	4			
3D	CAMRY	LE	2001	L4	2.2L	3	S	[illegible]	[illegible]
4D	CAMRY	SE	2007	L4	2.4L	5	S	24.9	193.0
5D	CAMRY	LE	2006	L4	2.4L	5	D	15.4	234.3
6D	CAMRY	LE	2007	L4	2.4L	5	S	25.3	138.1
7D	CAMRY	XLE	2005	L4	2.4L	5	D	29.8	167.1
8D	CAMRY	XLE	2001	V6	3.0L	4	S	32.5	158.1
9D	CAMRY	LE	2005	V6	3.0L	5	D	43.6	268.2
10D	CAMRY	LE	2007	V6	3.5L	6	S	30.9	217.8
11D	CAMRY	XLE	2005	V6	3.0L	5	S	25.7	236.0
12C	CAMRY	XLE	2007	V6	3.5L	6	S	22.1	148.6

29.8 lbs. | 167.1lbs.

V6

Brake Test Data Table: http://www.nhtsa.gov/staticfiles/nvs/pdf/NHTSA-Toyota_vehicle_characterization.pdf, p. 34

OUR ANALYSIS OF TOYOTA'S SOFTWARE

13 chapters

- Vehicle code analysis

+1 summary

- Case-specific analysis

>750 pages

+ appendices…

That's a GRANDE coffee!

#KillerApps

~~THE SOFTWARE DEFECTS IN DETAIL~~

"Highly Confidential"

- Even I don't have a copy of my expert report!

"Source Code Protective Order"

- The contract I signed to see the code is also secret!

BUT a transcript of my testimony is around…

- Try "bookout toyota barr"

BARR group

TEST SPACE EFFECTIVELY INFINITE

Lots of ways for the software to malfunction

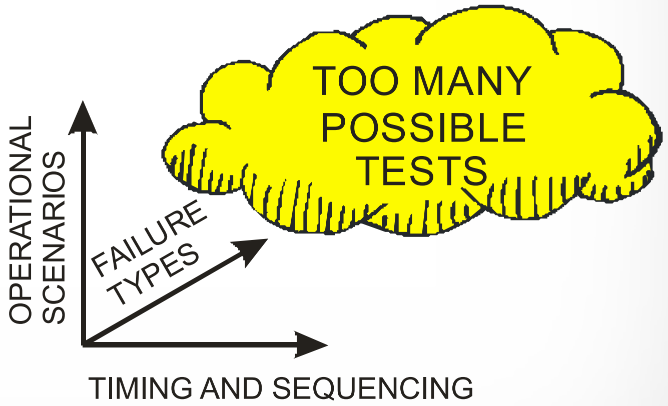
And a malfunction can begin in lots of states

- Precise timing of events
- Internal software states
- Vehicle operating states

  Cruise on or off?

  Accel at 5% or 50%?

  Failing O_2 sensor?
- Driver reactions



#KillerApps

IN-VEHICLE TESTING

2005 & 2008 Camry

- Fault-injection test
- Dynamometer

Defects confirmed

- Gaps thru fail safes

  And a defect in one!

- Loss of throttle control

  Violation of a NHTSA safety standard

  Via a single point of failure (a bit flip!)

BARR group

Caveat: Not of the actual dynamometer or test vehicle.

#KillerApps

TOYOTA'S TESTING

Each model "*goes through a driving test for over 400,000 miles. … In this we have never confirmed an instance of unintended acceleration.*" – *Toyota*

- BUT first 4,000 buyers do more testing in first week

  In more cars in more weather with more drivers etc.

U.S. fleet of 2002-2007 Camrys: ~1 billion hrs/yr!

– *NASA, Appendix A, FN 24*

Testimony: http://democrats.energycommerce.house.gov/sites/default/files/documents/Interview-Ogawa-Kishi-Toyota-2010-3-18.pdf

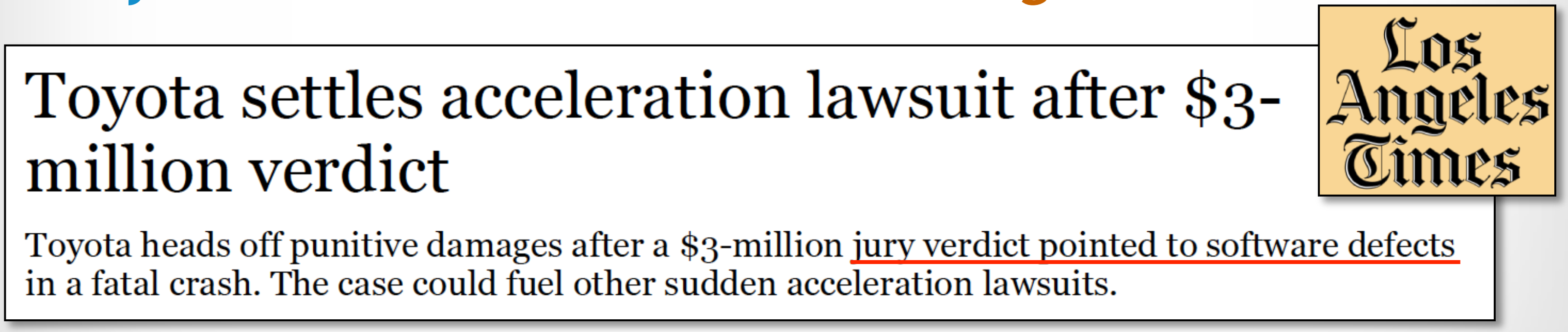
THE JURY VERDICT

Damage award

- Toyota to pay Mrs. Bookout: $1.5M
- Toyota to pay Mrs. Schwarz' estate: $1.5M

Punitive finding

- Toyota acted with: *"reckless disregard"*



Los Angeles Times

Toyota settles acceleration lawsuit after $3-million verdict

Toyota heads off punitive damages after a $3-million jury verdict pointed to software defects in a fatal crash. The case could fuel other sudden acceleration lawsuits.

Source: http://www.latimes.com/business/autos/la-fi-hy-toyota-damages-20131026,0,1605124.story

#KillerApps

TOYOTA LITIGATION SUMMARY

Plaintiff	Court	My Role	Status	Amount
Saylor	CA	-	settled Feb '11	$10M
Van Alfen	U.S.	report Jul '12	settled Dec '12	private
U.S. Class	U.S	report Jul '12	settled Dec '12	up to $1.5B
Bookout	OK	testimony Oct '13	verdict Oct '13	$3m + ??
Vance	WV	retained	settled Dec '13	private
St. John	U.S.	report Apr '13	in talks Dec '13	*
Canada Class	ON	retained	settled Mar '14	~$150M
Criminal	U.S.	-	settled Mar '14	$1.2B
new cases	*various*	*ongoing*	*still being filed*	**$3B+**

* One of approximately 400 injury cases in settlement talks now.

Yet no remedy…

BARR group

#KillerApps

ACKNOWLEDGEMENTS

Nathan Tennies

Dan Smith

Nigel Jones

NASA's Toyota Review Team

Dr. Koopman Carnegie Mellon University

Carl Muckenhirn
Steve Loudon
Doug Denney

#KillerApps

SAFETY FUTURE

Google's code driving Toyota's code…

THE SOFTWARE SAFETY LANDSCAPE

Voluntary Standards

IEC 61508
implement
reviews
standard
IS026262
Functional Safety
integrated and validated.
ISO
IEC
MISRA

Regulation/Oversight

DO-178B

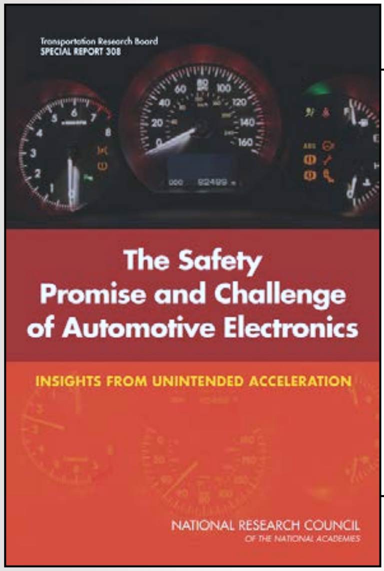
Litigation?

#KillerApps

AUTOMOTIVE SAFETY

Modern vehicles are networks of computers

- Brake-by-wire, collision avoidance, etc. emerging…



Transportation Research Board
SPECIAL REPORT 308

The Safety Promise and Challenge of Automotive Electronics

INSIGHTS FROM UNINTENDED ACCELERATION

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

"**FAA exercises far greater oversight** of the verification and validation of designs and their implementation" **than NHTSA**.

"**NHTSA does not set its own design and implementation standards, nor does it demand that manufacturers follow third-party standards** to guide design, development, and evaluation processes such as testing of software code"

BARR group

TRB Special Report 308: http://www.nap.edu/catalog.php?record_id=13342

#KillerApps

HOW DO WE MAKE OUR SYSTEMS SAFER?

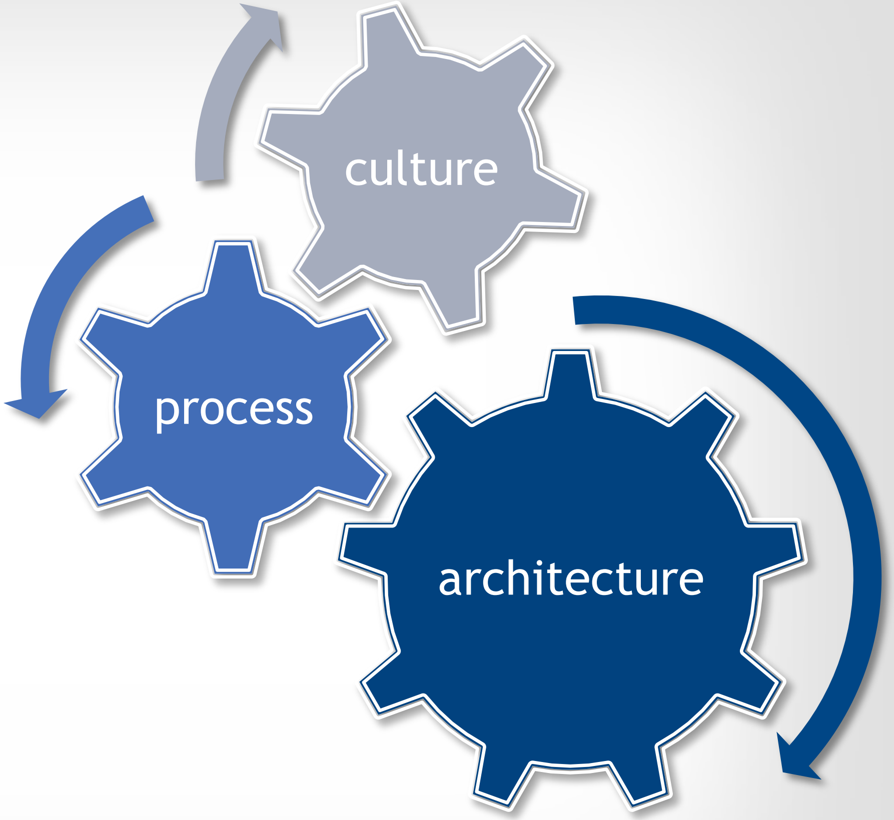
No quick fix

But certainly NOT…

- “It can’t be software”

Sunshine is needed

- Informed oversight
- Less code confidentiality



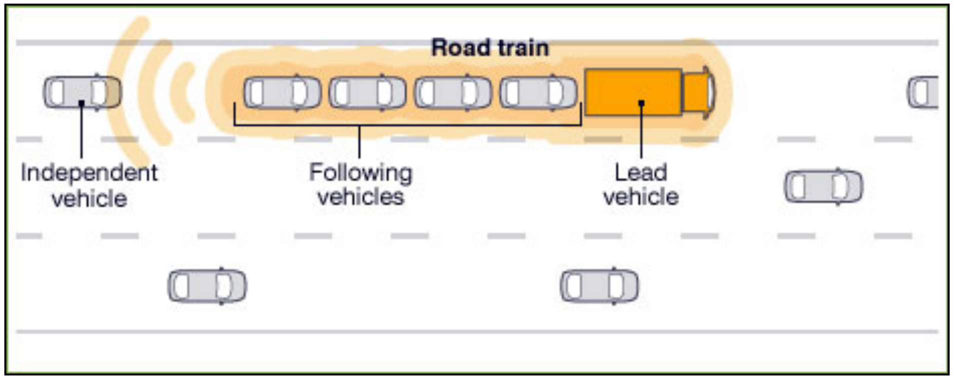
BARR group

#KillerApps

IMAGINE A WORLD…

What if you could wave a magic wand?

"Self-driving cars and smart highways for all"



Everyone is safer—on average—in and around cars!

Accidents now caused by engineering mistakes

Better/safer drivers lose advantages

BARR group

#KillerApps

WHEN WILL IT BE SAFE?

http://www.barrgroup.com/killer-apps/