KILLER APPS
Embedded Software’s Greatest Hit Jobs

April 1, 2014
Michael Barr
@embeddedbarr
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 helps companies make their embedded systems safer and more secure.

@barrgroup #embedsys #safety #security
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.”

PATRIOT MISSILE FAILURE

February 25, 1991
- 28 U.S. soldiers dead; 98 wounded
- Single deadliest incident for U.S.

GAO: Software Problem Led to System Failure at Dhahran, Saudi Arabia
THE PATRIOT SOFTWARE BUG

Two versions of system time

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

7.5s: 000000000000000000000111.1000000000000000000000002

Increasing inaccuracy...

<table>
<thead>
<tr>
<th>uptime (h)</th>
<th>error (s)</th>
<th>shift (m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.0034</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>.0275</td>
<td>55</td>
</tr>
<tr>
<td>20</td>
<td>.0687</td>
<td>137</td>
</tr>
<tr>
<td>100</td>
<td>.3433</td>
<td>687</td>
</tr>
</tbody>
</table>

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.
THERAC-25 SYSTEM OVERVIEW

Installations in 5 U.S. and 6 Canadian facilities

 Thousands of treatments as intended, but...

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

ONE OF THE THERAC-25 BUGS

---

**Hkeeper**

- **Lmtchk**: If Class3=0, 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$\text{mal}

---

**Task**

**Tphase**

- **Set Up Test**: During set, increment Class 3 on each cycle. Check F$\text{mal}$. If F$\text{mal}$=0 system is consistent then set Tphase=2 for Set Up Done.

---

**Class3 Global rolls every 256**

---

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”

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

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
AUTOMOTIVE SOFTWARE TRENDS

Image: http://gearheads.org/understanding-the-brain-at-the-heart-of-your-car/
Honda recalls nearly 350k Odyssey minivans over unintended braking

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.
Toyota adds “electronic throttle” ~2002 models

NHTSA investigates “UA” complaints (5 times)

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

Then a high profile crash...

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


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

“Saylor”
28 Aug ’09
UNINTENDED ACCELERATION

What is unintended acceleration?

- Acceleration the driver did not purposely cause

> 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!

ELECTRONIC THROTTLE CONTROL

- Engine Software
- Driver Controls
- Combustion
- Cruise
- Accelerator
- Fuel
- Throttle control
- Air
- Spark
POSSIBLE SOURCES OF ACCELERATION

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

Driver error
- “Pedal misapplication”

Software malfunction

~30% of models recalled
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%)

Could driver errors explain the jump?

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

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.

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

Environmental/Usage Factors

Factors held ~constant.

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

Camry (see page 42)

ES 300 Series (see page 43)

Tacoma (see page 44)

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”
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 found no evidence of ETCS-i causing UAs. 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.

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

Toyota had to produce source code and design docs.

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

* Saylor (and some other early plaintiffs) did not look into software.
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
Custom-built room
- No Internet
- No phones

Layered security
- Guard station
- More... I can’t say!

At a secret address...

Photo: Not of the actual source code room.
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
Speed estimates
- Skid start ~50mph
- At impact ~25mph

Agreed she braked
- Parking brake too?

150’ skid mark
- Way too long!
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.”

Consumer Reports Video: http://youtu.be/VZZNR9O3xZM
At large throttle openings (35 degrees (absolute) or greater), if the driver pumps the brake pedal, 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.

<table>
<thead>
<tr>
<th>Vehicle Information</th>
<th>Brake Hold at Wide Open Throttle</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Engine</td>
</tr>
<tr>
<td></td>
<td>Config. Displacement Fwd Speeds</td>
</tr>
<tr>
<td>Veh. ID.</td>
<td>Model</td>
</tr>
<tr>
<td>1D</td>
<td>CAMRY</td>
</tr>
<tr>
<td>2D</td>
<td>CAMRY</td>
</tr>
<tr>
<td>3D</td>
<td>CAMRY</td>
</tr>
<tr>
<td>4D</td>
<td>CAMRY</td>
</tr>
<tr>
<td>5D</td>
<td>CAMRY</td>
</tr>
<tr>
<td>6D</td>
<td>CAMRY</td>
</tr>
<tr>
<td>7D</td>
<td>CAMRY</td>
</tr>
<tr>
<td>8D</td>
<td>CAMRY</td>
</tr>
<tr>
<td>9D</td>
<td>CAMRY</td>
</tr>
<tr>
<td>10D</td>
<td>CAMRY</td>
</tr>
<tr>
<td>11D</td>
<td>CAMRY</td>
</tr>
<tr>
<td>12D</td>
<td>CAMRY</td>
</tr>
</tbody>
</table>

**Brake Test Data Table:** [http://www.nhtsa.gov/staticfiles/nvs/pdf/NHTSA-Toyota_vehicle_characterization.pdf](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!
“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”
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

Too many possible tests
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!)*

*Caveat:* Not of the actual dynamometer or test vehicle.
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

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”

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
# KILLER APPS

## TOYOTA LITIGATION SUMMARY

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

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

Yet no remedy...
ACKNOWLEDGEMENTS

Nathan Tennies
Dan Smith
Nigel Jones

NASA’s Toyota Review Team

Dr. Koopman
Carl Muckenhirn
Steve Loudon
Doug Denney
SAFETY FUTURE

Google’s code driving Toyota’s code...
THE SOFTWARE SAFETY LANDSCAPE

Voluntary Standards
- IEC 61508
- ISO
- IEC
- MISRA

Regulation/Oversight
- DO-178B
- FDA 510(k)

Litigation?
Modern vehicles are networks of computers

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

“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”

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
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
WHEN WILL IT BE SAFE?

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