

Companion blog to the book Better Embedded System Software by Phil Koopman at Carnegie Mellon University

Pages


[Home](#)

Automotive software defects

Cyclic Redundancy Code/Check (CRC) Resources

About Me

- 

 **Phil Koopman**

I work with self-driving car safety and more generally with dependable embedded systems. I teach at Carnegie

Mellon University.

As with any blog, these posts often contain speculative and partially formed thoughts, and should not be interpreted as a fully considered opinion unless stated otherwise.

These blog posts are copyrighted and are not to be reproduced or rehosted.

Key pages:

Academic home page at CMU

Embedded Software Blog

Safe Self-Driving Car Blog

Checksum and CRC Blog

[View my complete profile](#)

Ad

Ad

Ad

Ad

Blog Archive

- ▶ 2024 (1)
- ▶ 2022 (2)
- ▶ 2021 (3)
- ▶ 2020 (1)
- ▶ 2019 (2)
- ▶ 2018 (8)
- ▶ 2017 (21)
- ▶ 2016 (25)
- ▶ 2015 (10)
- ▼ 2014 (28)
 - ▶ November (1)
 - ▼ October (2)
 - Safety Culture
 - A Case Study of Toyota
Unintended Acceleration and...
- ▶ September (3)
- ▶ August (2)
- ▶ July (1)

Investigations into potential causes of Unintended Acceleration (UA) for Toyota vehicles have made news several times in the past few years. Some blame has been placed on floor mats and sticky throttle pedals. But, a jury trial verdict was based on expert opinions that defects in Toyota's Electronic Throttle Control System (ETCS) software and safety architecture caused a fatal mishap.

This talk will outline key events in the still-ongoing Toyota UA litigation process, and pull together the technical issues that were discovered by NASA and other experts. The results paint a picture that should inform future designers of safety critical software in automobiles and other systems.

Bio:

Prof. Philip Koopman has served as a Plaintiff expert witness on numerous cases in Toyota Unintended Acceleration litigation, and testified in the 2013 Bookout trial. Dr. Koopman is a member of the ECE faculty at Carnegie Mellon University, where he has worked in the broad areas of wearable computers, software robustness, embedded networking, dependable embedded computer systems, and autonomous vehicle safety. Previously, he was a submarine officer in the US Navy, an embedded CPU architect for Harris Semiconductor, and an embedded system researcher at United Technologies. He is a senior member of IEEE, senior member of the ACM, and a member of IFIP WG 10.4 on Dependable Computing and Fault Tolerance. He has affiliations with the Carnegie Mellon Institute for Software Research (ISR) and the National Robotics Engineering Center (NREC).

=====

I am getting an increasing number of requests to do this talk in person, both as a keynote speaker and for internal corporate audiences. Audiences tell me that while the video is nice, an in-person experience of both the presentation and small-group follow-up discussions has a lot more impact for organizations who need help in coming to terms with creating high quality software and safety critical systems. If you are interested please get in touch for details: koopman@cmu.edu

Other info:

- [Download copy of full-resolution video file set of talk](#), Box.com 340 MB .zip file of a web directory with interactive split-screen viewing format. Experts only! Please do not ask me for support -- it works for me but I don't have any details about this format beyond saying to unzip it and open Default.html in a web browser.)
- [Mirror of full resolution video talk download](#) (dropbox.com of same files as on box.com)
- One or more of these download sites might be blocked by company networks, so if you get an error message please try both links at home. If they still don't work, send me an e-mail and I'll see what I can do.
- [Download medium-bit-rate 720p video](#) from CMU server (.mp4; 124MB)

All materials (slides & video) are licensed under [Creative Commons Attribution BY v. 4.0](#).

Please include "Prof. Philip Koopman, Carnegie Mellon University" as the attribution.

If you are planning on using the materials in a course or similar, I would appreciate it if you let me know so I can track adoption. If you need a variation from the CC BY 4.0 license (for example, to incorporate materials in a situation that is at odds with the license terms) please contact me and it can usually be arranged.

=====

at [October 03, 2014](#)



Labels: [safety](#), [Toyota UA](#)

- [June](#) (4)
- [May](#) (4)
- [April](#) (4)
- [March](#) (4)
- [February](#) (2)
- [January](#) (1)
- [2013](#) (12)
- [2012](#) (10)
- [2011](#) (18)
- [2010](#) (41)

Labels

[agile methods](#)
[architecture](#)
[automotive software](#)
[book](#)
[CAN](#)
[career](#)
[coding style](#)
[compilers](#)
[concurrency](#)
[CRC/checksum](#)
[defects](#)
[dependability](#)
[documentation](#)
[economics](#)
[Edge Case Research](#)
[editorial](#)
[EEPROM](#)
[embedded C](#)
[embedded networks](#)
[error detection](#)
[Essays](#)
[exceptions](#)
[Free Sample Chapter](#)
[globals](#)
[hardware](#)
[Internet of Things \(IoT\)](#)
[interrupts](#)
[management](#)
[math](#)
[metrics](#)
[ML validation](#)
[open source](#)
[optimization](#)

3 comments:

kredit agya November 11, 2014 at 2:38 PM

i ask for permission to copy this article

[Reply](#)



Phil Koopman November 11, 2014 at 9:39 PM

The slides and video are both released under CC BY 4.0

<https://creativecommons.org/licenses/by/4.0/>

That gives you (and everyone else) permission to copy with some pretty minimal restrictions. If for some reason the restrictions don't work for you, please contact me with the specifics of the situation.

[Reply](#)

Karim Naqvi September 11, 2015 at 1:37 PM

Wonderful, Phil! I had not noticed you posted this presentation. I'll point students in my embedded class to the video, and of course to your text which, unfortunately, I'm not using this fall. The presentation is a bit of a challenge: fairly dense slides, with much jargon. Still, a great resource, and thank you.

[Reply](#)



Enter Comment

Please send me your comments. I read all of them, and I appreciate them. To control spam I manually approve comments before they show up. It might take a while to respond. I appreciate generic "I like this post" comments, but I don't publish non-substantive comments like that.

If you prefer, or want a personal response, you can send e-mail to comments@koopman.us. If you want a personal response please make sure to include your e-mail reply address. Thanks!

[Newer Post](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)

Static Analysis Ranked Defect List

Crazy idea of the day: Static Analysis Ranked Defect List. Here is a software analysis tool feature request/product idea: So many times we...



Don't use macros for MIN and MAX

[outsourcing](#)

[peer reviews](#)

[process improvement](#)

[project management](#)

[quality](#)

[real time](#)

[recall](#)

[requirements](#)

[research](#)

[risk management](#)

[robustness](#)

[safety](#)

[security](#)

[self-driving cars](#)

[SQA](#)

[static analysis](#)

[system design](#)

[testing](#)

[time keeping](#)

[tools](#)

[Toyota UA](#)

[traceability](#)

[tutorial](#)

[updates](#)

[USI](#)

[versioning](#)

[watchdog timer](#)

Report Abuse

Follow Me On Twitter

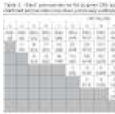
Follow [@PhilKoopman](#)

Top Posts

- [Embedded Training Videos](#)
 - [Top Five Embedded Problems](#)
 - [Toyota Unintended Acceleration](#)
 - [Best CRC Polynomials](#)
 - [Embedded Software Cost](#)
 - [Cyclomatic Complexity](#)
 - [Watchdog Timer Use](#)
 - [EEPROM Corruption](#)
-



It is common to see small helper functions implemented as macros, especially in older C code. Everyone seems to do it. But you should ...



What's the best CRC polynomial to use?

(If you want to know more, see my Webinar on CRCs and checksums based on work sponsored by the FAA.) If you are looking for a lightwei...

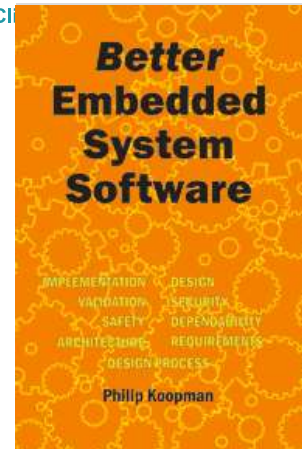


A Case Study of Toyota Unintended Acceleration and Software Safety

Oct 3, 2014: updated with video of the lecture Here is my case study talk on the Toyota unintended acceleration cases that have been in ...

Book Info

Click



[Click here for book description.](#)

This book gives concrete approaches to achieving better embedded software in 29 different areas.

[Click here for Free Sample Chapter](#)

Other Embedded Blogs

[Safe Autonomy](#)

[Checksum and CRC Central](#)

[Jack Ganssle](#)

Reader Locations



Pages

[Automotive software defects](#)

[Cyclic Redundancy Code/Check \(CRC\) Resources](#)

Search This Blog