Food for Thought™

An e-newsletter published by
Software Quality Consulting, Inc.

March 2010 , Vol. 7 No. 2
[Text-only Version]

Welcome to ***Food for Thought***™, an e-newsletter from **Software Quality Consulting**. I've created free subscriptions for my valued business contacts. If you find this newsletter informative, I encourage you to continue reading. Feel free to pass this newsletter along to colleagues by clicking on the **Forward Email** link at the bottom of this email. If you've received this newsletter from a colleague and would like to subscribe, please click this **Enter New Subscription** link. If you don't wish to receive this newsletter, click the **SafeUnSubscribe**™ link at the bottom of this newsletter, and you won't be bothered again.

Your continued feedback on this newsletter is most welcome. Please send your comments and suggestions to **info@swqual.com**.

In this issue

In **This Months' Topic**, I discuss continuing problems with software in the automotive industry.

Regular features to look for each month are:

- **Monthly Morsels**
  Hints, tips, techniques and reference info related to this month's topic
- **Calendar**
  Conferences, workshops, and meetings of interest to software engineers, QA engineers and anyone interested in software development

This month's topic

Running On Code - Part II

Finding the Root Cause of Toyota's Sudden Acceleration Issue

In my last newsletter, I discussed problems associated with complex software used to control cars. Late model cars have over **100 million lines of code** and are likely to have as many as **600,000 defects** that haven't been found.

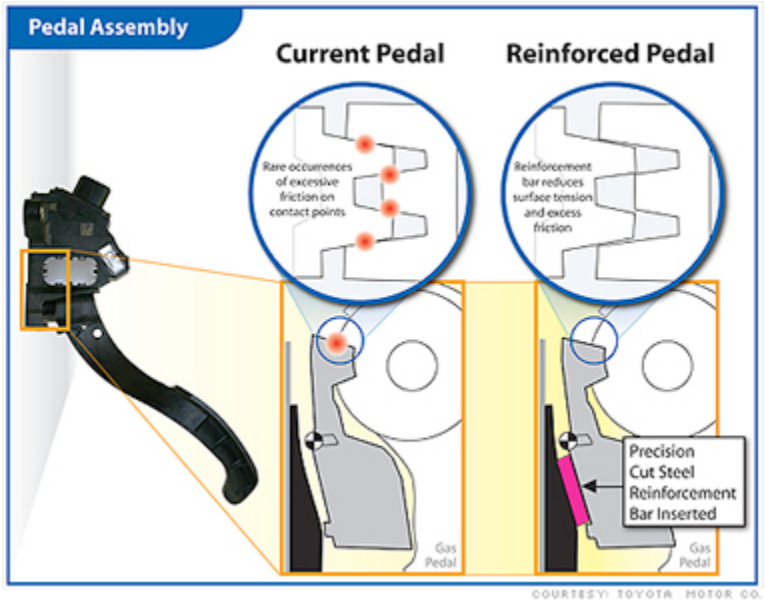
This on-going problem serves to illustrate that all software is defective and defective software *could be* one of the underlying root causes of Toyota's sudden acceleration problem.

For reasons that are unclear, Toyota has been unable to find the **real root cause** of the sudden acceleration problem. While there is clearly a lot at stake here – lawsuits, recall and repair costs, and lost sales are estimated at $5 billion – this problem has escalated to become a major safety issue for Toyota and the automotive industry in general.

Here's a recap of Toyota's attempts at finding the **root cause:**

- First, Toyota announced late last fall that the root cause was **improperly installed floor mats** that became wedged behind the gas pedal. This claim was promptly dismissed by several customers who reported sudden acceleration in cars that didn't have floor mats or had floor mats that were clearly not wedged behind the gas pedal.

- Then, on February 1 st, Toyota announced the root cause was the **gas pedal assembly** and they quickly came up with a re-designed gas pedal assembly as shown below:



Toyota then began replacing gas pedals on several million recalled vehicles and they denied that electronics or software was involved. Toyota owners of vehicles affected by the recalls dutifully brought their cars in for the required repairs.

- Within the past week, however, there has been increasing evidence that the gas pedal assembly is **not** the root cause. There have been at least seven unconfirmed reports from Toyota owners who have had the prescribed recall repairs performed on their vehicles and have since reported further episodes of sudden acceleration. Both Toyota and the National Highway Traffic Safety Administration (NHTSA) are currently investigating these events.

Making the problem worse, there is now evidence that the sudden acceleration problem is not confined to models Toyota originally identified. A Prius owner in California has recently reported his car exhibited sudden acceleration. His car sped up to 94 MPH with “both feet on the brake.” The man was able to call 911 while this was

happening and a state trooper managed to position his cruiser in front of the Prius and helped slow the car down. Fortunately, no one was injured.

As can be seen from these events, **Toyota has not yet found the real root cause** or causes of the sudden acceleration problem – or if they have, they are not saying what it is. A key aspect of performing an effective root cause analysis is collecting as much information about the problem as possible and using that information to lead you to the real root cause. More on this in a bit…

Other recent events have raised more concerns with the approach Toyota has taken to find the root causes of this issue and the response (or lack thereof) from NHSTA:

- **Event Data Recorders**

  Many late model cars have an airplane-like black box called an event data recorder (EDR). An EDR is a small, virtually indestructible box similar to black boxes used on commercial airplanes. The EDR records vehicle and engine speed as well as brake, accelerator and throttle position and other data that can help determine causes of accidents.

  Up until this week, Toyota has refused to provide access to the encrypted information captured by the event data recorder and there was only one computer in North America that was able read data from these event recorders. "Last week, Toyota acknowledged it has only a single laptop available in the U.S. to download its data recorder information because it is still a prototype, despite being in use since 2001 in Toyota vehicles. Three other laptops capable of reading the devices were delivered this week to NHTSA for training in their use, Toyota said, and 150 more will be brought to the U.S. for commercial use by the end of April." [2]

  According to an Associated Press report [2], Toyota has

frequently refused to provide key information sought by crash victims and survivors and only provides this information when requested by legal means. In fact, the company policy "… is to download data only at the direction of law enforcement, NHTSA or a court order." When EDR information is provided, much of it is redacted. Toyota has in the past chosen to settle lawsuits out of court rather than provide EDR information. A reasonable conclusion one can draw from this behavior is that they are hiding something.

Honda also refuses to make their black box data available while GM, Ford, Chrysler, and Nissan do make their event data recorder information routinely available.

- **Refuting Independent Investigations**

  Toyota has publically refuted allegations by Prof. David Gilbert of Southern Illinois University aired on ABC News on February 22, 2010. Prof. Gilbert demonstrated how a Toyota Avalon and a Lexus could experience sudden acceleration by intentionally short-circuiting specific signals.

  Toyota recently issued a press release [4] which stated:

  > "Toyota and Exponent [an engineering consulting firm hired by Toyota] have provided Professor David Gilbert of Southern Illinois University with the results of their thorough evaluations of his demonstration of apparent 'unintended acceleration' in Toyota and Lexus vehicles as described in his Preliminary Report and in his testimony at recent Congressional hearings. In evaluating Professor Gilbert's claims, Exponent also analyzed the footage of Professor Gilbert's appearance on ABC News on February 22,

2010."

> "Toyota has also supplied the results of these evaluations to the appropriate Congressional Committees. The analysis of Professor's Gilbert's demonstration establishes that he has reengineered and rewired the signals from the accelerator pedal. This rewired circuit is highly unlikely to occur naturally and can only be contrived in a laboratory. There is no evidence to suggest that this highly unlikely scenario has ever occurred in the real world. As shown in the Exponent and Toyota evaluations, with such artificial modifications, similar results can be obtained in other vehicles." [1]

The fact that Prof. Gilbert was able to cause sudden acceleration provides one very important piece of information – **electronics can cause the event**. Prof. Gilbert also demonstrated that when this event happens, the event does not appear in the car's diagnostic code.

- **Ineffective Oversight by NHSTA**

  NHTSA is the agency in the US that regulates the automobile industry and investigates safety issues. It was recently learned that NHSTA **does not have any software engineers on their staff.** Given the widespread use of software in cars today, much of it safety-critical, it seems that NHSTA should:

  - hire software engineers and SQA staff as soon as possible,
  - require all auto manufacturers to have event data recorders, just like airplanes, and
  - require EDR information to be stored in a manner that is

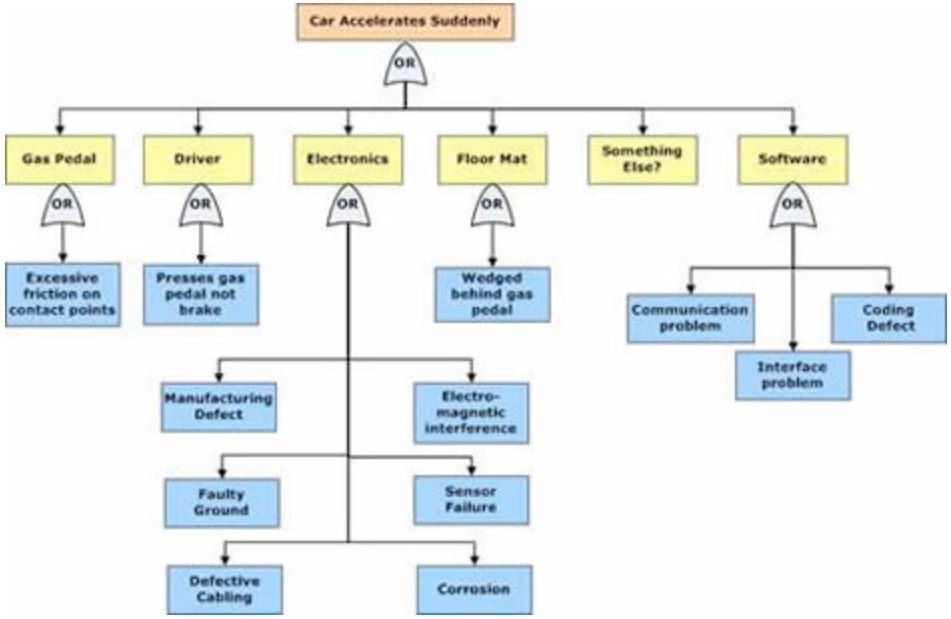
readily accessible, so that data can be used to identify the potential root causes of future accidents

Representative Gene Green (D-TX) plans to introduce legislation requiring NHSTA to mandate EDRs on all new cars and trucks. This legislation also should require that information not be encrypted as Toyota's presently is.

Performing Root Cause Analysis

Root cause analysis has been used to investigate and understand dozens of major disasters including airplane crashes, the Space Shuttle Challenger explosion, and many other catastrophic accidents.

It is a relatively straightforward task to create a fault tree (also call a Why Tree) for the sudden acceleration problem. Using only information available on-line and in published reports, a fault tree for the problem might look like this…



The trick in learning how to apply this tool effectively is to:

- focus on what is physically possible, rather than what seems reasonable
- use qualitative and quantitative data to rule things out or rule them in
- assume reports submitted by customers are reliable and accurate

If Toyota engineers are to be successful in finding the real root causes, they need to be pursuing every branch of this fault tree as well as identifying additional branches. Once they do this, they can then drill down each branch and identify ways in which events and/or failures may cause sudden acceleration. With this information, the engineers can develop solutions to prevent the problem from occurring again.

- **Learn how to perform Root Cause Analysis for customer-reported problems.**

Creating a Safety Case

A safety case is an effective tool for demonstrating that an organization has taken all reasonable steps to ensure their software is safe for its intended use. A simple safety case has three parts:

Claim:	A statement about the software you are making
Arguments:	Why you believe the claim is true
Evidence:	Information that directly supports the arguments

Safety cases are routinely used in mass transit systems primarily in Europe and are often used to provide confidence that software systems are safe.

If a safety case were prepared for Toyota's throttle control software,

it might look something like this:

Claim:	**Throttle control software is safe.**
Arguments:	1. The throttle control software was developed to meet the following safety requirements [enumerate them] and complies with the following international standards [enumerate them]. 2. The throttle control software requirements have been documented, reviewed, and approved [cite document #] 3. The throttle control software design specifications have been documented, reviewed and approved. [cite document #s] 4. The throttle control software has been thoroughly tested according to a documented and approved test specification. [cite document#] 5. The throttle control software test results have been reviewed and approved and the software is determined to be acceptable for use. [cite document #] 6. A Risk Assessment of the throttle control software was performed and the results documented [cite document #]
Evidence:	1. The Requirements Trace Matrix shows that every requirement in the throttle control software SRS has been tested. 2. The Validation Report shows the results of

	validation testing of the throttle control software. 3. The Risk Management Report for the throttle control software shows what risks were considered and how they were resolved.

The Bottom Line....

The unfolding Toyota saga is far from over. The inability or unwillingness to find or admit to the real root cause is fostering doubt and fear among loyal Toyota owners and among all consumers. While this problem is affecting Toyota right now, it is very likely that similar problems will appear in other cars, just based on the amount of software embedded in today's cars.

If nothing else, this episode has served to shed light on the fact that some of the **100 million lines of code** in today's cars are potentially safety-critical. Safety-critical software used in regulated industries such as medical devices, nuclear power, and avionics is generally safe mostly because that software is developed using rigorous development processes.

Perhaps Congress needs to require that safety-critical automotive software be regulated...

'Til next time...

Every month in this space, you'll find additional information related to this month's topic.

References

1. http://pressroom.toyota.com/pr/tms/toyota/toyota-consumer-

safety-advisory-102572.aspx.

2. AP IMPACT: Toyota secretive on 'black box' data By CURT ANDERSON and DANNY ROBBINS (AP), March 5 2010.

3. Bensinger, K. and Vartabedian, R., "Toyota's fix is a bust, owners claim", LA Times, March 03, 2010.

4. Toyota Press Release - Comprehensive Analysis Raises Concerns About Gilbert Congressional Testimony, ABC News Segment.

Every month you'll find news here about local and national events that are of interest to the software community…

- **Software Quality Calendar**

  There are many organizations that sponsor monthly meetings, workshops, and conferences of interest to software professionals. **Find out what's happening...**

- **Workshops Offered by Software Quality Consulting**

  Software Quality Consulting offers workshops in many topics related to software process improvement. **Get more info...**

Software Quality Consulting provides consulting, training, and auditing services tailored to meet the specific needs of clients. We help clients fine-tune their software development processes and improve the quality of their software products. The overall goal is to help clients achieve Predictable Software Development™ – so that organizations can consistently deliver quality software with promised

features in the promised timeframe.

To learn more about how we can help your organization, **visit our web site** or **send us an email**.

I hope this newsletter has been informative and helpful. Your comments and feedback are most welcome. **Send me your feedback...**

Thanks,

Steve Rakitin

info@swqual.com

Software Quality Consulting Inc.

Steven R. Rakitin
President

- **Consulting**
- **Training**
- **Auditing**

Phone: 508.529.4282
Fax: 508.529.7799

www.swqual.com
info@swqual.com