TAP TIMES

March 2017
Volume 8, Number 3

Focus on failures: Overlooking the obvious can be costly

Electronic component manufacturers and OEM users face an interesting dichotomy when dealing with electronic component failures.

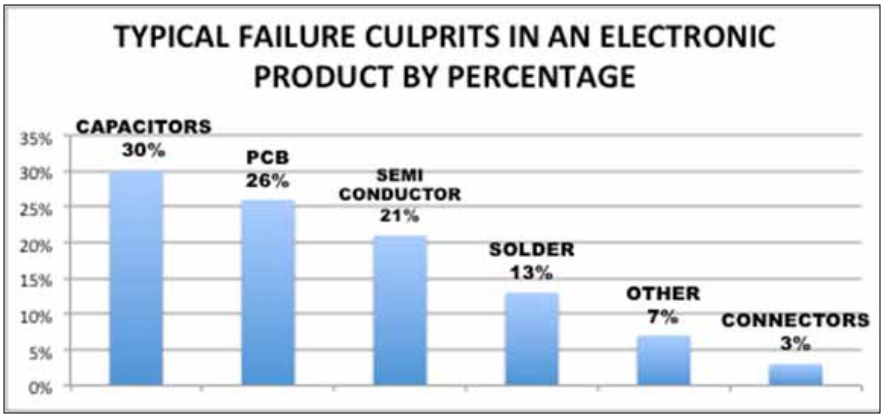
System complexity

Electronic system complexity, such as smaller IC feature sizes, smaller non-hermetic packages, long-life products, design re-use and challenges in component sourcing can lead to some difficult failure analysis and consequently require corrective actions.

Tom Terlizzi
GM Systems LLC
Kings Park, N.Y. 11754
gmsystems.com

"Failure culprits"

As shown in the figure (at right) there is typically a wide range of "failure culprits" which can occur during manufacture, development testing, and qualification or during use of an electronic product.



Most companies deal with failures either in their early developmental testing and "shake out" pre-production runs, in-process manufacturing or field failures in an expeditious and proactive manner.

There have been many cases, however, where failures have been neglected or just accepted due to time-to-market concerns, fear of bringing "bad news" to management, electronic system complexity and other challenges.

As we enter the era of "driverless cars," the 2014 recall by General Motors of ~2.5 million cars due to a faulty ignition switch comes to mind. A faulty ignition switch could accidentally turn the car off.

This causes loss of electrical power with loss of braking power, inability to steer and the disconnection of safety features such as air bag systems.

Switch detent plunger

The switch detent plunger is a part of the ignition switch designed to provide sufficient mechanical resistance to prevent accidental rotation. In the faulty ignition switches, the switch detent was insufficient. This allowed accidental rotation that turned off the engine. ***See next page***

Focus on failures (from 3)

Based on internal documents that have since been discovered, executives and engineers at General Motors knew about the defect in these ignition switch detent plungers, but failed to inform the government or consumers.

Due to the incidents associated with the faulty ignition switches in 30 million vehicles, General Motors has experienced a loss of over $4 billion in shareholder value.

Lessons learned
The root cause of GM's problems involved the faulty ignition switch not having enough torque, which enabled the ignition switch to move out of the "run" position.

A contributing cause, however, was a General Motors engineer's acceptance of a switch design that did not meet the minimum torque value.

Several years later, after the switch was redesigned with the correct torque, the part number was not changed, violating company procedure. This change caused confusion in the failure analysis, leaving engineers puzzled as to why there were no failures in the earlier years only in the later ones.

An additional contributing cause was that the engineers worked in "silos" and did not classify this failure as a safety concern since they were not aware that the air bags would not deploy in the "off" position.

It took 11 years to solve the problem
The General Motors board directed its law firm to investigate and find out why it took 11 years to resolve the faulty ignition problem.

Among the highlights:

• *Ensuring safety reporting lines are clear and reach to the top of the organization via a vice president for vehicle safety.*

• *Eliminating overlaps and gaps in departmental safety responsibilities.*

• *Reviewing policies and procedure, to make them more comprehensible and accessible.*

• *Provide adequate staffing for safety positions.*

• *Place greater attention on trend data and monitoring recalls of other manufacturers to identify learning.*

• *More rigorous engineering, investigation and product recall processes, with clearer deadlines and better records maintenance .*

• *Attention to safety culture development.*

A costly software failure
As early as 2003 Toyota had been aware of vehicle unintended acceleration (UA) problems, defined as "any degree of acceleration that the vehicle driver did not purposely cause."

See page 6

Focus on failures (from 4)

From 2005-2010 almost 15 million Toyota cars were recalled for UA problems due to "stuck accelerator pedals caused by floor mats," "sticking accelerator pedals" or to get an electronic upgrade with a brake override.

Stuck accelerator pedals (believed caused by Toyota floormats) led to a recall of nearly 15 million Toyotas. (Wikipedia)

Unexplained cases

There were still many UA cases of death or serious injuries, which could not be explained.

In 2011 the National Highway Traffic Safety Administration (NHTSA), and NASA released a report after a 10-month study, that found no electronic or software defects in the Toyota drive-by-wire throttle system or Electronic Throttle Control System (ETCS).

Not the end of the story

But the NASA and NHTSA report was not the end of the story.

In October 2013, the *Bookout vs. Toyota Motor Corp.* case ruled against Toyota and found that unintended acceleration could have been due to deficiencies in the drive-

See page 9

Focus on failures (from 4)

by-wire throttle system or Electronic Throttle Control System.

20-month study

The Barr Group after a 20-month study and an 800-page report on the ETCS source code testified that NASA had not been able to complete its examination of Toyota's ETCS and that Toyota did not follow best practices for realtime life-critical software.

A single bit flip caused by cosmic rays could provoke unintended acceleration, the study revealed.

Data overwritten

In addition, the run-time stack of the real-time operating system was not large enough. It was possible, the report found, for the stack to grow large enough to overwrite data that could cause unintended acceleration as well as over 81,514 issues in the code.

In March 2014, the U.S. Department of Justice announced a $1.2 billion ruling against Toyota related to unintended acceleration and associated practices in hiding defects in its vehicles.

See next page

Focus on failures (from 9)

This brings the total for these UA recalls, fines and settlements to over $1.6 billion.

Summary
The cases discussed show that OEMs must "focus on failures" early in the evaluation phase and design safety and quality into their products. The complexity of automotive electronics hardware and software is a major challenge. Unraveling cover-ups are costly.

If General Motors had redesigned their ignition switch with a increase in unit price of ~$1 and a tooling cost of ~$400,000, many lives would have been saved, and serious injuries would have been eliminated.

In addition, billions of dollars in losses would have been averted.

Stronger standards needed
NHTSA needs to enforce stronger automotive software standards for safety critical software design similar to the FAA's safety requirements for civilian aircraft (DO-178 standards).

A single loss of life or serious injury requires "failure is not an option" thinking.

See next page

Focus on failures (from 10)

The author

Mr. Terlizzi is vice president at GM Systems LLC, a management and technology consulting firm. For over 30 years, he has designed and developed power management systems, single board computers, microelectronic devices, thick and thin film hybrids and other products for military, aerospace and consumer markets.

He received a BEE from City College of New York and an MSEE from NYU-Polytechnic. He writes a blog for EDN Online and has published several articles, papers and tutorials at international conferences.

Article sources

1. "Root-Cause Failure Analysis of Electronics," Bhanu Sood Test Services and Failure Analysis (TSFA) Laboratory Center for Advanced Life Cycle Engineering (CALCE)
University of Maryland, SMTA Philadelphia, March 14, 2013.
2."GM Ignition Switches" Consumersafety.org (https://www.consumersafety.org/products/gm-ignition-switches/)
3. Consumer Alert: GM Ignition Switch Recall Information. Safercar.gov. April 10, 2014.
cars. Detroit Star. May 17, 2014.
4. GM fined $35mn for delays in recalling faulty
5. L. Hurley, General Motors settles last bellwether ignition-switch cases. Reuters. Sep. 5, 2016.
6. In re. General Motors LLC Ignition Switch Litigation.
7. United States v. General Motors Company, Sep.17, 2015. Updated Jan. 29, 2016.
8. G.M. Internal Investigation Report, N.Y. Times, June 5, 2014
9. "GM Ignition Switch Debacle – Safety Lessons," Sep 8, 2014 Aerossurance
10. "A Case Study of Toyota Unintended Acceleration and Software Safety," Prof.Phil Koopman, Carnegie Mellon University, Sep. 18, 2014.
11. "An Update on Toyota and Unintended Acceleration," Oct. 26, 2013, Michael Barr.
12. "Software bugs found to be cause of Toyota acceleration death". Phil Baker, (2013-11-04). San Diego
13. "Acceleration Case: Jury Finds Toyota Liable". EE Times. Junko Yoshida, Oct. 23, 2013.
14. "Toyota Enters Settlement Talks Over Sudden-Acceleration Lawsuits". Business Week. Bloomberg. Paul Barrett,Dec. 16,2013.
15. "Toyota to pay $1.2B to settle criminal probe", Eric Tucker and Tom Krishner, Associated Press March 19, 2014
16. Failure Analysis when Failure Is not an Option! Tom Terlizzi, VP, GM Systems, April 24, 2015,http://www.planetanalog.com/author.asp?section_id=3121&doc_id=563929-