the Availability Digest
www.availabilitydigest.com

Unintended Acceleration and EMI

April 2010

Does the absence of a detectable fault prove the absence of a design defect?

Is electromagnetic interference (EMI) with automobile engine computers the cause of so many sudden, unintended acceleration (SUA) incidents? That is the controversy now raging in the public domain as auto manufacturers scramble to reassure nervous customers about the safety of their vehicles. The engine computers (electronic control units, or ECUs) control throttle settings, fuel/air mixture ratios, and transmissions in order to satisfy increasingly stringent fuel economy and emission standards. Sometimes, unfortunately, these computers misbehave. When that happens, the computers often leave no evidence trail. How can an ECU design defect be corrected if you can't detect the fault?

Manufacturers (most recently Toyota) claim that their automobiles undergo extensive EMI testing that has demonstrated no link between SUA and EMI. Critics, including engineering professionals, counter that the tests have not been comprehensive enough. Judges and juries have consistently rejected attempts to link SUA with EMI, ruling that the hypothesis is scientifically unreliable.

Yet SUA incidents have surged since the widespread introduction of ECUs in automobiles a decade ago. In March, the Los Angeles times reported 102 deaths attributed to Toyota SUA incidents. SUA is clearly a serious problem, no matter the cause. So what is the solution?

Is EMI the Culprit?

Unfortunately, we may never know. If radiation were to affect a computer, the effect would be transient and would leave no footprints. But wouldn't exhaustive testing show the problem?

How Should We Test EMI Susceptibility?

Let's put some numbers on realistic testing. Let us assume that the average car over the last decade has been driven for 100,000 miles (some cars are new with lower mileage while others are older with higher mileage). The eight million cars that Toyota recently recalled have therefore logged about 800 billion miles.

Industry analysts have estimated that there have been about 10,000 reports of SUA incidents. Assuming that these are all Toyota-related (which they are not), this means that an SUA incident occurs every 80 million miles of driving, on the average. To do enough testing to have a hope of causing just one SUA incident will require driving 800 cars in an EMI-intensive environment for 100,000 miles each. This is clearly not feasible.

And what is an EMI-intensive environment? EMI covers a broad range of frequencies from AM radio stations to microwave towers. There have been many suggestions on the source of radiation, assuming that it is a problem. What is agreed is that the EMI source must be pretty

strong because the ECUs, their wiring, and their transponders are purportedly well-shielded to prevent EMI problems.

Possible Sources of EMI

However, EMI theories abound. Following are some of the suggested EMI sources that could impact a car's ECU.

The Car

Some point out that the automobile itself is a major source of EMI. Significant EMI is generated whenever a current in the local wiring of the automobile suddenly changes. This can happen for instance, whenever headlights or brake lights turn on or off. Have you ever been bothered by excessive noise in your car radio because of faulty spark-plug wiring? This is an example of EMI.

Power Transmission Lines

CNN recently reported a study investigating the potential link between high-voltage overhead power lines and SUA incidents. The study plotted the location of SUA incident reports against the power-grid topology. The report found that an alarming number of SUA incidents – about 39% - occurred in the densest areas of transmission lines, even though these concentrations were well outside of highly-populated and well-traveled areas. Furthermore, the study found many SUA incidents appeared to happen just after a car passed under the power lines (but it was not reported whether this was statistically significant).

Car Washes

Another suspected source of EMI, interestingly, is car washes. It seems that a disproportionate number of SUA incidents have happened in car washes. Car-wash operators have complained about this for years. The thought is that moisture gets on the wiring and acts as a conductor for EMI.

Mobile Electronics

The airlines have been plagued by EMI. When cell phones, laptops, and other electronic devices first came into prominence, pilots occasionally found that their sensitive avionic instruments malfunctioned. Some experimentation with passengers pointed the finger at EMI from mobile devices. Now, all electronic equipment must be turned off during the critical takeoff and landing phases of all flights.

Cosmic Radiation

Even fault-tolerant NonStop processors may experience a similar problem. When a NonStop processor misbehaves (and is replaced automatically by another processor), HP often returns the processor to the factory to be tested. A large proportion of these processors (some say 80%) are determined to be fine. One theory is that occasionally a particle from outer space (like a Gamma ray) knocks an electron out of orbit in a semiconductor and causes it to have a transient failure. This isn't EMI, but it is analogous.

NHTSA Tests

In 2008, the NHTSA (the US National Highway Traffic Safety Administration) reported after testing a 2007 Lexus ES 350:

> "Magnetic fields were introduced in proximity to the throttle body and accelerator pedal potentiometers and did result in an increase in engine revolutions per minute (RPM) of up to 1,000 RPM, equivalent to a cold-idle engine RPM level."

So it can happen.

One outcome to note is that if EMI, a wayward cosmic particle, or any other random event disrupts the processing function in an ECU, *anything* can happen. The result is totally nondeterministic. Intended actions can be disrupted, and failsafe logic can fail. Arguments that the software in the ECU protects against such happenings is totally invalid. Even having independent, redundant ECUs that compare their results before issuing commands doesn't solve the problem. As we have pointed out many times in the Availability Digest, all this does is to move back the barrier to perfect operation. It never eliminates it.

No wonder the experts claim that testing has not been rigorous enough. It is probably impossible to structure a reasonable test that will affirm or deny the responsibility of EMI in these incidences. The NHTSA, aided by NASA and the National Academy of Sciences, has now decided to reopen its investigation as to whether EMI could be a factor. However, at this point, the NHTSA asserts that it has no reason to believe that EMI is causing SUA incidents.

So What To Do?

Toyota has undergone a massive recall of over eight million cars worldwide (over five million of them in the U.S.) to fix place mats and to modify accelerator pedals to correct the SUA problem that owners are experiencing. Maybe this will eliminate such incidents, and the argument will be over. But if the incidents continue, even at a slower pace, what is the next step?

Electronic Brake Override

A solution currently being implemented by Toyota and other manufacturers (such as Chrysler and Nissan) is a brake override feature. This is appearing in new cars, and Toyota is retrofitting some older cars going back to 2007. The feature gives priority to braking over throttle actions. If sensors are calling for both acceleration and braking, braking will win. This will solve the floor-mat problem. But will it solve an EMI problem? After all, the brake override feature will be implemented by the same ECU that may be affected by EMI.

Let us say that the Toyota fixes eliminate 90% of the SUAs. An SUA incident will still happen about every one billion miles. Isn't this probability so small that we can ignore it? Probably not. It is estimated that Americans drive 3 trillion miles per year. If SUA incidents happen once every one billion miles, we can expect about 3,000 SUA incidents a year. How many of these will be fatal? Thus, this probability cannot be ignored.

At some point, we might have to conclude that the cause of SUA may never be determined and that there will always be the possibility, though remote, that an SUA incident can happen. We will have to accept that s**t happens, and we will just have to deal with it. How do we do that?

Mechanical Brake Override

Clearly, there must be some failsafe method to control the car in the event that the ECU goes haywire. This method must be totally independent of the ECU – we don't want the failsafe mechanism to experience the same failure that the ECU is experiencing.

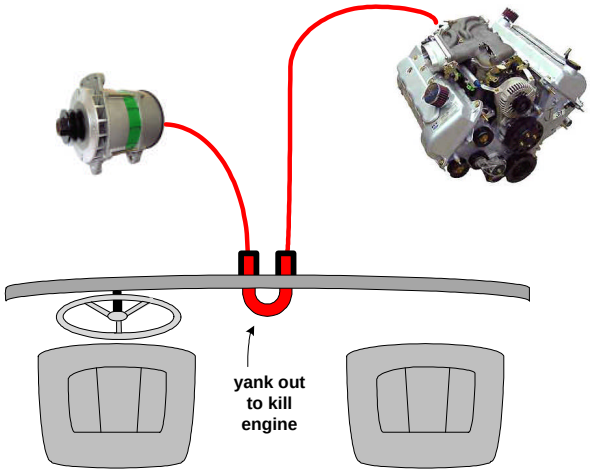
One very good suggestion is to have a mechanical linkage that gives priority to braking. If the brake is depressed, the linkage forces the throttle to close, slowing down the engine (goodbye to racing car starts by holding the brakes while the engine revs up).

This is an excellent solution, but it is still not totally failsafe since there is a remote possibility that the mechanical linkage might fail. If the linkage can't be easily tested, how will the owner know that his linkage has failed and that it will not be there when he needs it?

The override mechanism must use nothing that can fail – electronics, relays, or mechanical linkages.

The Ultimate Failsafe Solution

One such solution is a manual fuse that disconnects the generator from the engine, ensuring that the engine will stop. Think of a red ring on the dashboard that you can pull and break the electrical circuit from the engine's electrical power source – the generator – to the engine's spark plugs. This will stop the engine no matter what.



It is hard to see how this solution can fail. Or have we simply moved the availability barrier back even further without eliminating it?

Summary

We in the IT community are painfully aware that gremlins hide in computer systems. Whether the problem is EMI, software bugs, operator error, or HAL trying to take over Discovery One (remember the movie "2001: A Space Odyssey"?), we must find absolutely failsafe methods to identify and correct safety-critical computer faults. Of course, the ultimate failsafe method will depend upon no electronics or mechanical linkages that themselves can fail.

Is our "manual fuse" solution truly absolutely failsafe? No. It still depends upon human action. What about the poor soul who has rented a car and hasn't familiarized himself with that funny red knob on the dashboard? Can we ever really eliminate the availability barrier? Probably not. We can only keep moving it back a little at a time. The problem will always be with us.

Just wait until steer-by-wire is introduced!

Post Script

The April 14th issue of USA Today reported that at least 131 Toyota owners experienced unintended acceleration after their recalled vehicles were repaired at dealerships. The saga continues.

Acknowledgements

Material for this article was taken from the following sources:

Toyota's Worst Nightmare: EMI-Linked Unintended Acceleration, *Gearlog*; March 24, 2010.
Could electronics be what's causing runaway cars?, *USA Today*; February 23, 2010.
Toyota's Acceleration Issue Due to Electronics, Experts Say, *The Epoch Times*; March 28, 2010.
Sudden Unintended Acceleration in Runaway Cars: Is Electro-Magnetic Interference Causing it?, *ATCA*; February 26, 2010.
US: Toyota refutes EMI effects on acceleration, *Automotive World*; March 24, 2010.
Electronics Experts Discuss EMI in Sudden Acceleration Incidents, *Interference Technology*; March 25, 2010.
Possible Electronics Causes for Sudden Unintended Acceleration, Professor Raj Rajkumar (blog), Carnegie Mellon University; February 23, 2010.
Brake Overrides: The Devil in the Details, Professor Raj Rajkumar (blog), Carnegie Mellon University; February 19, 2010.
Feds seek help with Toyota Scrutiny, *USA Today*; March 31, 2010.