NASA Engineering and Safety Center Study of Unintended Acceleration in Toyota Vehicles

Mike Kirsch – Principal Engineer and NASA Study Lead

NASA Engineering and Safety Center
Langley Research Center
Hampton, VA

March 3, 2011
NASA analysis and testing did not find evidence that malfunctions in the electronic throttle control caused large unintended accelerations, as described by some consumer reports.
NASA Support to DOT

• NASA began discussions with NHTSA in March 2010.

• The scope was to determine if there are design vulnerabilities in the Toyota electronic throttle control that could possibly cause unintended acceleration that can be realistically expected to occur in consumer’s use of these vehicles.
  ✓ Vulnerabilities that lead to unintended acceleration and,
  ✓ Are realistically expected to occur in consumers use

• NASA formed a team with engineering experts in systems, avionics, software, electromagnetic interference, and human factors.
# Project Organization

## Systems Engineering
- DFRC Edwards, CA
- GSFC Greenbelt, MD

### Project Management
- LaRC Hampton, VA

### Software Analysis and Test
- ARC Moffett Field, CA
- DFRC Edwards, CA
- GSFC Greenbelt, MD
- JPL Pasadena, CA
- TMC Torrance, CA
- TMC San Jose, CA

### Hardware Analysis and Test
- GSFC Greenbelt, MD
- KSC Titusville, FL
- LaRC Hampton, VA
- VTRC East Liberty, OH

### Human Factors
- ARC Moffett Field, CA

### Consumer Report Analysis
- ARC Moffett Field, CA
- DFRC Edwards, CA
- GSFC Greenbelt, MD
- NHTSA Washington DC

### Electromagnetic Interference
- Chrysler Ann Arbor, MI
- GRC Cleveland, OH
- JSC Houston, TX
- MSFC Huntsville, AL
Guiding Questions

• What specific conditions, both internal and external, are necessary for these failure conditions to occur?
• Are those conditions evident in the reported cases?
• What physical or electronic evidence does the failure produce?
• What are the expected ranges in severity?
• Could the failure have any effect on other interfaces, such as braking system?
Study Approach

• The NASA team received and evaluated theories from outside NHTSA and NASA.
• The NASA Team evaluated consumer reports and warranty return data, while studying how the electronic throttle control works.
• The Model Year 2005 Toyota Camry was identified as a vehicle to study in depth.
• From the NHTSA consumer report data, the majority of the consumers described large throttle openings with degraded braking that did not leave a trace or diagnostic trouble code.

The NASA study focused on identifying failure modes that could result in large throttle openings, may not generate a diagnostic trouble code, or leave physical evidence.
Technical Evaluation

• The technical strategy was to analyze the Toyota electronic throttle control system to understand how it is supposed to work and then explore how it might cause unintended acceleration.

• The NASA team assembled and tested critical electronic throttle control components as a system including the accelerator pedal, throttle body, and electronic control module to understand how the system might cause an unintended acceleration.

• The NASA software team modeled the code, ran the code on simulators, and subjected the code to automated code checkers.
• The NASA team had access to vehicles purchased by NHTSA from consumers with symptoms of unintended acceleration.

• The NASA team performed electromagnetic interference testing on these same vehicles obtained from consumers that had filed consumer reports with NHTSA.
Findings
• No Toyota vehicle was identified that could naturally and repeatedly reproduce large throttle opening unintended acceleration effects for evaluation by the NESC team.
NASA Findings

• Safety features are designed into the Toyota throttle control to guard against large throttle opening unintended acceleration from single and some double throttle system failures.
  • Multiple independent safety features include detecting failures and initiating safe modes, such as limp home modes and fuel cut strategies.
The NESC study and testing did not identify any electrical failures in the electronic throttle control that impacted the braking system as designed.

- At large throttle openings (35 degrees (absolute) or greater), if the driver pumps the brake, then the power brake assist is either partially or fully reduced due to loss of vacuum in the reservoir.
- NHTSA demonstrated that a MY 2005 Camry with a 6 cylinder engine travelling at speeds up to 30 mph can decelerate at better than 0.25g with 112 lbf on the brake while the throttle is open up to 35 degrees (absolute), with a depleted vacuum assisted power brake system.
For pedal assembly failures to create large unintended throttle openings, failures need to mimic valid accelerator pedal signals.

- Two failures in the precise resistance range, to create the exact circuit configuration in the correct time phase are necessary for this functional failure to occur. Failure to meet these restrictive conditions will generate a diagnostic trouble code (DTC).
- Some first failures in dual failure scenarios of Hall Effect accelerator pedal systems might not be detectable by the electronic control module or via diagnostic data to the on board diagnostic interface.
- A review of the warranty data does not indicate an elevated occurrence of pedal or electronic control module related diagnostic trouble codes relative to unintended acceleration consumer reports.
NASA Findings

- Destructive physical analysis of a failed pedal assembly from a consumer vehicle with a diagnostic trouble code found a tin whisker had formed a 248 ohm resistive short between VPA1 and VPA2.
- A second tin whisker of similar length was growing from a 5 volt source terminal adjacent to a pedal signal output terminal, but had not made contact with any other terminals. Inspection of “non-failed” potentiometer pedals revealed tin whiskers present in similar locations as the failed pedal.
  - Destructive physical analysis shows the Denso Hall Effect accelerator pedal sensor is protected against the tin whisker resistive shorts.
  - The CTS pedal provides physical separation between the VPA1 and VPA2 thereby removing one component of the dual fault scenarios.
Vehicle testing of a MY 2005 Toyota Camry demonstrated that a 248 ohm short between VPA1 and VPA2 results in different vehicle responses depending on the sequence of operations following the fault.

In all cases, releasing the accelerator pedal closes the throttle, and brakes are fully operational.
• Functional failures of the cruise control can result in 0.06 g’s, or 2.12 kph/s, acceleration and may not generate a diagnostic trouble code; however, there are multiple methods for cancelling or turning off cruise control.
• Functional failures of idle speed control, transmission control, vehicle stability control, and throttle control may result in throttle openings of less than 5 degrees above idle and may not generate a diagnostic trouble code. Per a NESC team request:
  • NHTSA demonstrated that a MY 2005 Camry with a 6 cylinder engine can be held in a stopped condition with a brake pedal force of approximately 8.5 lb$f$ with throttle openings up to 5 degrees above idle.
• Comprehensive electromagnetic compatibility testing well beyond recommended certification levels was performed on six different Toyota consumer vehicles to determine EMC levels that could have an effect.

• No throttle control vulnerabilities from EMC radiated testing were identified that would result in throttle increase.
NASA Findings

• Extensive software testing and analysis was performed on Toyota 2005 Camry L4 source code using static analysis, logic model testing, recursion testing, and worse case execution timing.

• With the tools utilized during the course of this study, software defects that unilaterally cause a unintended acceleration were not found.
Observations

Observations are conclusions from our testing and analysis that are may be outside of the study scope, or are unsubstantiated by evidence from the field
Resolution of a UA depends on driver awareness of mitigations, driver response, UA situations (e.g., open highway, crowded parking lot), and other factors (e.g., environmental).

Some VOQs indicate that some drivers may not know or understand the vehicle response for the hazard controls at their disposal and how to use them. For example:

- Shifting to neutral with the resulting high engine speed will not harm the vehicle.
- Pumping the vacuum assist brakes can decrease their effectiveness.
- Turning the vehicle off while driving may require a different sequence than when the vehicle is stopped and will not lock the steering wheel.
- Shifting patterns vary between vehicles and within a vehicle may require different motions to get to neutral when in modes other than drive and reverse.
• During testing, the limp home mode safety feature closed the throttle when the brake was pressed. When the brake can override the throttle command it provides a broad defense against unintended engine power whether caused by electronic, software, or mechanical failures.
NASA Observations

- Failures of safety critical systems in the ETC do not provide the same driver information as failures that occur in the safety critical brake systems.
  - A unique red ‘warning light’ is illuminated for the brake system, while only a generic, multi-purpose check engine light occurs for off-nominal ETC conditions.
NASA Observations

- The Government-mandated (Environmental Protection Agency) DTCs are for emission control and are not mandated to cover safety critical failures.
NASAs Observations

- Vehicles that are operated with an active accelerator pedal sensor fault, either with the MIL on or off, may be susceptible to the effects of second faults, leading to possible unintended accelerations.
  - NHTSA and NASA evaluated 188 Swift Market Analysis Response Team (SMART) data sets from TMC complaint vehicles and found no proof that the second fault is occurring and resulting in UA in those vehicles.
• While not resulting in a design vulnerability, the MY 2005 Camry source code required unique code inspection tools, and manual inspections due to:
  • The TMC software development process uses a proprietary developed coding standard.
  • Industry standard static analysis tools provide automated code inspections based upon industry standard code implementations.
NASA Observations

- There are no methods for capturing pre-event software state and performance following a UA event either on the vehicle or as a diagnostic tool.
• The available incident reporting databases are valuable for identifying potential vehicle symptoms related to UA events.
  • Voluntary reporting systems may not allow for accurate quantitative estimates of incident rates or statistical trends.
A review of HF literature related to UAs indicates that pedal misapplication remains an identified cause of some UAs.

- It is not possible to accurately estimate from available survey and laboratory data how frequently this error is an underlying cause.
NASA Observations

• Given that driver errors such as pedal misapplications are best characterized as low-probability random process events, it is difficult to study them in a controlled laboratory environment (e.g., human-in-the-loop driving simulation studies).
  • Manipulations that might be performed to increase the observed frequency might also compromise the ability to generalize the findings under consumers’ use of the vehicle.
Design features, such as sport shifter and push button stop, might compromise the driver’s ability to recover from a UA event.

- Such features may be indicative of broader driver-vehicle integration issues and therefore may merit further consideration.
It is recommended that NHTSA consider whether additional study, government regulation, or policy is warranted based on the findings and observations within this report.

- Controls for managing safety critical functions, as currently applied to the railroad, aerospace, military and medical sectors, warrant consideration.
Summary
Executive Summary

• NASA detailed analysis and testing did not find evidence that malfunctions in electronic throttle control caused large unintended accelerations, as described by some consumer reports.

• NASA found a way that the electronic throttle control can fail, that combined with driver input, can cause the throttle to jump to 15° open, but consumer reports of this condition is very low and it leaves evidence of occurrence.

• NASA found ways that the electronic throttle control can fail that results in small throttle openings up to 5°.