
	NASA Engineering and Safety Center Technical Assessment Report	Version: 1.0
Title:	National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation	Page #: 1 of 179

Technical Support to the National Highway Traffic Safety Administration (NHTSA) on the Reported Toyota Motor Corporation (TMC) Unintended Acceleration (UA) Investigation

January 18, 2011

WARNING: This document is SENSITIVE BUT UNCLASSIFIED (SBU). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552) or other applicable laws or restricted from disclosure based on NASA policy. It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with NASA policy relating to SBU information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized NASA official (see NPR 1600.1).

	NASA Engineering and Safety Center Technical Assessment Report	Version: 1.0
Title: National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation		Page #: 13 of 179

4.0 Executive Summary

The NASA Engineering and Safety Center (NESC) was requested by the National Highway Traffic Safety Administration (NHTSA) to study Toyota Motor Corporation (TMC) Unintended Accelerations (UAs). The goal of the study was to determine if there are design and implementation vulnerabilities in the Toyota Electronic Throttle Control System Intelligent (ETCS-i) that could cause UAs and whether those vulnerabilities, if substantiated, could realistically occur in consumers' use of these vehicles. TMC introduced the ETCS-i in the 2002 model year (MY) Camry to replace the mechanical linkage between the accelerator pedal and the throttle valve. The ETCS-i has electronic position sensors at the pedal and throttle, an actuator motor at the throttle, wiring, and additional electronic circuitry and software in the Engine Control Module (ECM) as shown in Figure 4.0-1.

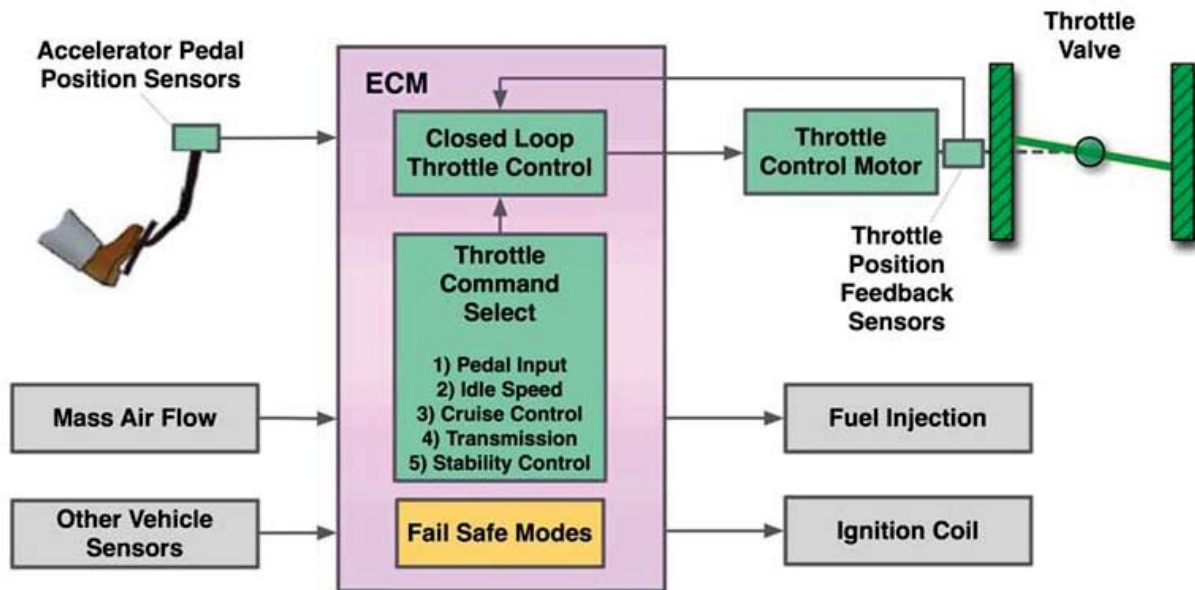



Figure 4.0-1. TMC ETCS-i

The ECM manages engine systems including the throttle valve, fuel injection, ignition, and emissions. The throttle valve is the primary control for engine speed and power by limiting the amount of air entering the engine. The electronic fuel injection system within the ECM maintains the proper air to fuel ratio based on the mass airflow and other sensor signals. Since ECM control of factors, other than air input (e.g., fuel injection and ignition spark) is optimized for engine performance, off-nominal setting of fuel injection and ignition factors does not produce significantly higher engine speed and power. Therefore, the ETCS-i control of the throttle valve was the main focus of this study in determining potential electronic causes of UA.

While electronic control systems may reduce the likelihood of mechanical failures, they can also potentially introduce anomalous modes not present with those mechanical systems. The NESC team examined the TMC ETCS-i system for the existence of such potential electronic

	NASA Engineering and Safety Center Technical Assessment Report	Version: 1.0
Title: National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation		Page #: 14 of 179

vulnerabilities or failure modes that could result in a UA as described by domestic consumer reports of events in the NHTSA Vehicle Owners' Questionnaire (VOQ) system.

The NESC team extensively studied the NHTSA VOQ dataset. Reported UAs are rare events. Typically, the reporting of UAs is about 1/100,000 vehicles / year or 1 in 1.4 billion miles. Of 426,911 total VOQ reports NHTSA received from calendar years 2000 to 2010 for all vehicle makes and models, there were 9698 identified as UA events based on expert review and analysis. Of these, 3,054 were for TMC vehicles.


The NESC team did not observe an increase in VOQ reports coincident with the introduction of ETCS-i on all TMC models. Some models show no effect and some models only indicate a small increase, while others show a slight decline in the number of reports received. However, there was an increase in UA VOQs coincident with publicity.

The VOQ records included 831 UA reports for Camry, and the MY 2005 Camry was selected by the NESC team for detailed analysis. Other Camry MYs, including 2002 and 2007, were compared alongside the MY 2005 to validate areas identified. VOQ reports were examined in detail and segregated into categories based on the symptoms reported which included causes traceable to normal characteristics of the vehicle design, problems identified in manufacturer technical service bulletins (TSBs), acknowledged driver actions, and other likely known causes including the floor mat and sticking pedal recall issues.

The NESC team review of VOQ data revealed that over one-half of the reported events described large (greater than 25 degrees) high-throttle opening UAs of unknown cause. In many cases the operator also reported that the brakes were ineffective at controlling the vehicle (i.e., an apparent loss of braking occurred). However, no evidence of a failure in either the ETCS-i or brake system typically was reported as having been found following these events. The NESC team determined that a large (greater than 25 degree) relative throttle valve opening would be required to produce this type of UA.

The NESC team applied a top-down systems engineering approach that explored the critical functions in the electronic throttle control, how the system might defend against failures (fail-safe design features), and if the system has vulnerabilities. The team:

- a) Had unrestricted access to the ETCS-i design, design engineering, drawings, schematics, software source code, and VOQ vehicles acquired by NHTSA.
- b) Studied whether the unknown source of UA failure modes could be identified, linked to typical consumer use, and demonstrated through testing of vehicles associated with consumer reports (VOQ vehicles) or vehicle components.
- c) Used data provided by the VOQ reports to determine where a flaw might be, what might cause it, and how it would manifest itself in normal use.
- d) Focused on evaluating the conditions under which the ETCS-i could cause a UA and not generate a diagnostic trouble code (DTC).

	NASA Engineering and Safety Center Technical Assessment Report	Version: 1.0
Title: National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation		Page #: 15 of 179

This systems study concluded that the ETCS-i architecture has a tiered fail-safe approach with a prime system and a monitor system. The team identified five fail-safe modes that range from limited pedal control to complete engine shutdown if one or more failures is detected. Two system-wide functional defenses against UA were observed: a limp home mode that limits maximum throttle opening to approximately 18 degrees (15 degrees above nominal idle of 3 degrees) if one of the two pedal position sensors fail and a fuel cut mode that limits engine speed when the accelerator pedal indicates it is released. If either one of two accelerator pedal sensors indicates that the accelerator is not pressed, then the engine speed will be limited to a maximum of 2500 rpm by a fuel cut function independent of the throttle valve position.


Driver defenses against UAs in ETCS-i vehicles are similar to those in vehicles with mechanical throttles: apply brakes, shift to neutral, or turn the ignition off. The NESC team did not find an electrical path from the ETCS-i that could disable braking. If the driver pumps the brake at large throttle openings of 35 degrees (absolute) or greater, then the power brake assist is either partially or fully reduced due to loss of vacuum in the reservoir. Per NASA request, NHTSA demonstrated that a MY 2005 V6 Camry traveling at speeds up to 30 mph can be slowed at 0.25g deceleration with 112 pounds force (lbf)¹ on the brake while the throttle is open up to 35 degrees, even with a depleted vacuum assisted power brake system. NHTSA also demonstrated that a MY 2005 V6 Camry can be held at a stopped position with approximately 10 pounds of brake pedal force with simulated failures causing 5-degree throttle increase above idle.

The NESC team identified two hypothetical ETCS-i failure mode scenarios (as opposed to non-electronic pedal problems caused by sticking accelerator pedal, floor mat entrapment, or operator misapplication) that could lead to a UA without generating a diagnostic trouble code (DTC): specific dual failures in the pedal position sensing system and a systematic software malfunction in the main central processor unit (CPU) that is not detected by the monitor system.

The first postulated scenario for a UA caused by electronic failure requires two failures in the pedal position sensing system which mimic a valid accelerator pedal command and therefore bypass all fail-safe architectural features. For this functional failure to occur, two electrical failures resulting in extraneous current paths in the precise resistance range, to the exact circuit configuration, occurring in the correct time phase, are necessary. It should be noted that there are significant differences between the failure effects of potentiometer pedal sensors used before 2007 and Hall Effect pedal sensors used in MY 2007 and later.

During the evaluation of the software source code, multiple automated tools were used to analyze software logic paths that might lead to a UA. Critical throttle control functions were modeled to look for potential algorithm or logic issues that could lead to unintended throttle opening. The models were validated on benchtop simulators consisting of a pedal, ECM, and throttle assembly configured for test functionality.

¹ These are federally mandated minimum deceleration and maximum brake force values as described in Federal Motor Vehicle Safety Standard 135.

	NASA Engineering and Safety Center Technical Assessment Report	Version: 1.0
Title: National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation		Page #: 16 of 179

Examination of the code found that throttle control variables are protected from corruption by storing multiple copies. In addition, two parallel functional paths to control engine power exist.

Based on postulated failure modes and predicted system responses, numerous electrical system hardware failure modes were tested on benchtop simulators and on six vehicles purchased from consumers submitting VOQs. The six vehicles represented the three different generations of electronic throttle control and included both 4 and 6 cylinder versions. Software and hardware test scenarios were based on both a top-down understanding of the system design and a bottoms-up testing of the electronic sensor inputs and postulated electronics failures that may affect the throttle position.


Vehicle testing using a defective potentiometer accelerator pedal assembly from a VOQ vehicle with a resistive short, within a narrow range of values between the sensors outputs, identified a vulnerability that may compromise nominal limp home mode fail-safe operation on subsequent ignition key cycles and affect the malfunction indicator lamp (MIL) display and/or DTC generation under certain specific conditions.

Destructive physical analysis of this pedal assembly found tin whiskers², one of which had formed the resistive partial short circuit between the pedal signal outputs. A second tin whisker of similar length was also found in this pedal assembly that had not caused an electrical short. If a resistive short between the potentiometer accelerator pedal signal outputs exists, the system may be vulnerable to a specific second fault condition that could theoretically lead to UA. However, if resistive faults were occurring during normal use, DTCs would be expected from at least the first ignition key cycle and the following cycles that did not meet the specific criteria. Subsequent review of the warranty data does not support an observable failure signature of pedal-induced DTCs. Electrical measurements on six VOQ vehicles found no indication of the resistive paths necessary for this failure scenario.

The second postulated scenario is a systematic software malfunction in the Main CPU that opens the throttle without operator action and continues to properly control fuel injection and ignition. The Main CPU malfunction would be required to open the throttle beyond 5 degrees with the accelerator not pressed and leave no failure evidence (e.g., DTC). The NESC team examined the software code (more than 280,000 lines) for paths that might initiate such a UA, but none were identified.

To test the hypothesis that the electronics caused the UAs, the NESC team investigated the six VOQ vehicles for signs of failure modes. The team examined the VOQ vehicles for signs of

² Tin whiskers are electrically conductive, crystalline structures of tin that sometimes grow from surfaces where tin (especially electroplated tin) is used as a final finish. <http://nepp.nasa.gov/whisker/>

	NASA Engineering and Safety Center Technical Assessment Report	Version: 1.0
Title: National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation		Page #: 17 of 179

electrical faults, and subjected these vehicles to electro-magnetic interference³ (EMI) radiated and conducted test levels significantly above certification levels. The EMI testing did not produce any UAs, but in some cases caused the engine to slow and/or stall.

Consumer VOQ vehicle components were dissected in search of tangible evidence of design or manufacturing flaws, particularly those with the potential to create greater than 25 degrees unintended relative throttle openings that could impair power braking if the brakes were pumped.

Proof for the hypothesis that the ETCS-i caused the large throttle opening UAs as described in submitted VOQs could not be found with the hardware and software testing performed. There is a single failure mode found that, combined with driver input, can cause the throttle to jump to 15 degrees in certain conditions and may not generate a DTC. This failure effect can be removed by releasing the accelerator pedal or overridden by the braking system. For the small throttle openings, the NESC team found single failure modes within the ETCS-i that can result in throttle openings less than 5 degrees. These failures may result in high idle speed, hesitation, and surging as described in submitted VOQs and may not generate DTC, but can also be removed by releasing the accelerator pedal or overridden by the braking system.

Because proof that the ETCS-i caused the reported UAs was not found does not mean it could not occur. However, the testing and analysis described in this report did not find that TMC ETCS-i electronics are a likely cause of large throttle openings as described in the VOQs.

³ Electromagnetic interference (or EMI, also called radio frequency interference or RFI) is an unwanted disturbance that affects an electrical circuit due to electromagnetic radiation emitted from an external source. Webster's Online Dictionary. Various standards govern test levels for certification of immunity to interference for consumer and military products. These test levels are greater than those expected during product use to demonstrate margin.