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

January 18, 2011

Report Approval and Revision History

Approval and Document Revision History

NOTE: This document was approved at the January 13, 2011, NRB. This document was submitted to the NESC Director on January 19, 2011, for configuration control.

Approved Version:	Original Signature on File	1/19/11
1.0	NESC Director	Date

Version	Description of Revision	Office of Primary Responsibility	Effective Date
1.0	Initial Release	Michael T. Kirsch, NESC Principal Engineer, LaRC	1/13/11

REDACTION NOTE

Since public release of this report on February 8, 2011, the Agency has revised its redactions to the document to release certain material previously deemed confidential under U.S.C. § 30167. This document, which was posted April 15, 2011 to NHTSA's web site, replaces the one posted previously and contains the Agency's revised redactions.

Table of Contents

List of Figures

List of Tables

1.0 Notification and Authorization

Mr. Daniel Smith, Department of Transportation (DOT), Senior Associate Administrator for Vehicle Safety, requested an independent assessment to determine if there are design and implementation vulnerabilities in the Toyota Motor Corporation (TMC) Electronic Throttle Control System-Intelligent (ETCS-i) that could cause unintended acceleration (UA). For the purposes of this assessment, Mr. Smith is considered the primary stakeholder. Analyses and tests characterizing all identified areas of concern were performed and the NASA Engineering and Safety Center (NESC) team documented their findings, observations, and NESC recommendations in this report. The results of the study were transmitted to Mr. Smith and the National Highway Traffic Safety Administration (NHTSA).

This NESC activity was approved by the NESC Director on March 4, 2010. The Assessment Plan was approved by the NESC Review Board (NRB) on May 20, 2010. The Authority and Parties for this activity are documented in a Fully Reimbursable Space Act Agreement between the NHTSA and NASA, IA1-1045 approved April 12, 2010, and in a subsequent Partially Reimbursable Space Act Agreement, IA1-1081 approved August 13, 2010.

2.0 Signature Page

Submitted by:

Original Signature on File

Mr. Michael T. Kirsch Date

Significant Contributors:

Team Signature Page on File

Ms. Victoria A. Regenie Date

Mr. Michael L. Aguilar Date

Mr. Oscar Gonzalez Date

Mr. Michael Bay Date

Mr. Mitchell L. Davis Date

Dr. Cynthia H. Null Date

Mr. Robert C. Scully Date

Mr. Robert A. Kichak Date

Signatories declare the findings and observations compiled in the report are factually based from data extracted from Program/Project documents, contractor reports, and open literature, and/or generated from independently conducted tests, analysis, and inspections.

3.0 Team List

The NESC team, listed below, is comprised of core members with expertise in: Systems Engineering; Electronics; Failure Modes and Effects, and Reliability; Parts, Materials, and Processes; and Software. The consultants' expertise brings added value in the areas of Environmental, Mechanisms, and Human Factors.

Name	Position/Technical Discipline Team (TDT) Affiliation	Center/ Contractor
Core		
Mike Kirsch	Co-Team Lead	Langley Research Center (LaRC)
Oscar Gonzalez	Co-Team Lead-Avionics	Goddard Space Flight Center (GSFC)
Mike Aguilar	Software	GSFC
Davy Baker	Electronics	GSFC
Michael Bay	Systems Engineer	GSFC, Bay Engineering Innovations
Peter P. Berg	Systems Engineer	ARC, Stinger Ghaffarian Technologies (SGT, Inc.)
Joseph Castle	Systems Engineer	ARC, SGT, Inc.
Michael Crane	EMI Specialist Engineer	Marshall Space Flight Center (MSFC), Jacobs Engineering
Mitchell Davis	Electronics Engineer	GSFC
Doron Drusinsky	Software Engineer	Time Rover
Ed Gamble	Software Engineer	Jet Propulsion Laboratory (JPL)
Trevor Harmon	Software Engineer	Ames Research Center (ARC) Oak Ridge Associated Universities (ORAU)
Gerard Holzmann	Computer Science Fellow	JPL
Chris Iannello	Systems Engineer	Kennedy Space Center (KSC)
George Jackson	Avionics	GSFC
Jeremy Johnson	Systems Engineer	ARC, SGT, Inc.
Mary Kaiser	Research Psychologist	ARC
Robert Kichak	Power and Avionics	GSFC, MEI Technologies, Inc.
Henning Leidecker	Electrical Products and Components Failure Analysis Engineer	GSFC
Michael Lowry	Software Reliability, Scientist	ARC
Hirokazu Miura	Aerospace Engineer	ARC
Cynthia Null	Human Factors	ARC
Joe Pellicciotti	Mechanical Systems	GSFC
Christopher Regan	Systems Engineer	Dryden Flight Research Center

Name	Position/Technical Discipline Team (TDT) Affiliation	Center/ Contractor
		(DFRC)
Vicki Regenie	Systems Engineer	DFRC
Masoud Mansouri-Samani	Computer Scientist	ARC, SGT, Inc.
Dwight Sanderfer	Computer Engineer	ARC
Johann Schumann	Computer Scientist	ARC, SGT, Inc.
Robert Scully	EMI/EMC Engineer	Johnson Space Center (JSC)
Phil Tang	Electronics Engineer	KSC
Walter Thomas	Aerospace Engineer	GSFC
Omar Torres	Electronics Engineer	LaRC
Glenn Williams	Electronics Engineer	Glenn Research Center (GRC)
Administrative Support		
Diana Kerns	MTSO Program Analyst	LaRC
Terri Derby	Project Coordinator	LaRC, ATK
Erin Moran	Technical Writer	LaRC, ATK

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.

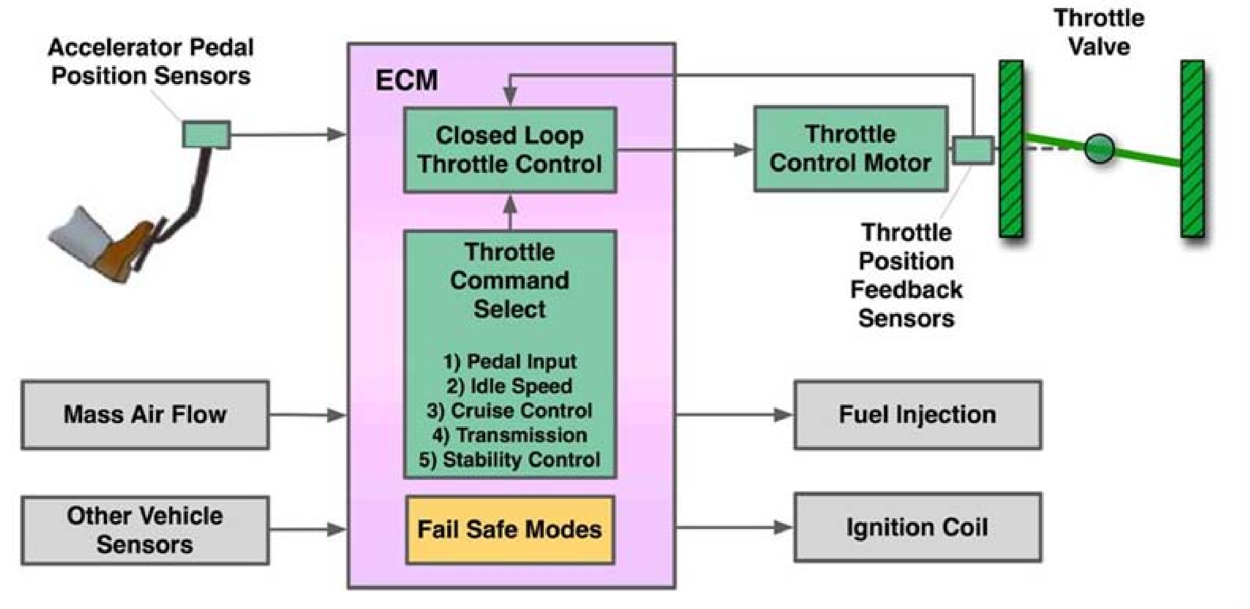


Figure 4.0-1. TMC ETCS-i

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 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).

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 (lb_f)[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.

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 whiskers[2], 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 electrical faults, and subjected these vehicles to electro-magnetic interference[3] (EMI) radiated

[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/

[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

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.

certification of immunity to interference for consumer and military products. These test levels are greater than those expected during product use to demonstrate margin.

5.0 Objective and Scope

The scope of this study was to determine if there are design and implementation vulnerabilities in the TMC ETCS-i system that could possibly cause UA that can realistically be expected to occur in consumers' use of these vehicles, and if so, whether these failure modes can be specifically identified and demonstrated through analysis and testing of vehicles or vehicle components. *For this report, findings are conclusions identified by engineering analysis validated by vehicle tests, and substantiated by consumer reports (VOQs), warranty data, field investigations, or physical/forensics of parts collected from the field. Observations are findings not directly related to the investigation that were discovered during the study. They can also be findings related to the investigation, but without physical evidence for substantiation.*

Standards and processes for managing and validating vehicle hazards and controls through design were not evaluated as part of this study.

When completed, the analysis and testing were expected to identify potential vulnerabilities (whether electronic, mechanical, or operator), if any, and answer the following questions:

1. What specific conditions, both internal and external, are necessary for these failure conditions to occur?
2. Are those conditions evident in the reported cases found in VOQs, warranty data, field investigations, and physical/forensic examination of parts collected from the field? If not, then is there other physical evidence that the conditions can realistically be expected to occur in the vehicle's normal operating environment?
3. What physical evidence does the failure produce? If none, then why?
4. What are the expected ranges in severity (e.g., throttle opening) and duration that could be caused by the failure?
5. Could the failure have any effect on other interfaces, such as braking system?[4]
6. What data, if any, are sent to and captured by the Event Data Recorder (EDR) and the ECM if a failure occurs? Will the identified failure inhibit the proper writing and storage of these data in the ECM?

    - The NESC team did not study the collection robustness or integrity of EDR data. The MY 2005 Camry EDR does not collect pre-event data.

5.1 Vehicle and MY Selection

The NESC team selected the MY 2005 Camry to concentrate *most of* their analysis and tests. Electronic throttle was introduced in Camry's beginning in MY 2002 and utilized potentiometer position sensors at both the accelerator pedal and throttle. MY 2004 through 2006 was the next

[4] NHTSA generated test procedures and supported tests to answer the question "Could the failure have any effect on braking system performance/effectiveness? If so, what effect?" that occurred in conjunction with NASA testing.

major hardware design evolution and utilized a potentiometer sensor at the accelerator pedal and a Hall Effect position sensor at the throttle. The current hardware version was introduced in MY 2007 and contains a Hall Effect sensor at both the accelerator pedal and the throttle. The MY 2005 Camry has interfaces and components that are similar to both earlier and later MYs, allowing it to span the design space. During this study, NHTSA provided NASA access to six vehicles obtained from consumers filing VOQs. The NHTSA's VOQ is a voluntary reporting system that allows any vehicle owner to register an incident, failure, crash, or injury involving their vehicle. The six vehicles span the three versions of electronic throttle control designs, including 4 and 6 cylinder versions. A detailed description of the VOQ vehicles is contained in table 6.8-1. The EMI/Electro-Magnetic Compatibility (EMC) testing included all six VOQ vehicles. Upon completion of the analysis, the intent was to compare possible vulnerabilities in the MY 2005 vehicle, identified in the analysis, and any susceptibilities identified during EMI/EMC testing, against the design characteristics of MY 2002 and 2007 platforms.

6.0 Analysis

6.1 Approach

The NESC team reviewed the NHTSA VOQs to understand the sequence of events or signature associated with the UAs. For the purposes of consumer VOQ review, UA is any vehicle acceleration unintended by the driver. The typical UA signature as described in a majority of VOQs requires the acceleration to be unexpected, occur for seconds to minutes, not generate a DTC or leave other physical evidence, and then not reoccur. A non-degrading intermittent fault would be consistent with this UA signature. The team evaluated VOQs and warranty data for trends or clues that could be traced to possible electronic caused UAs. The evaluation of the VOQs indicated the UAs were reported in a broad array of vehicles and more importantly with a variety of suspect electronic components, (e.g., different pedal types, different throttle types and different ECMs). Electronic problems are typically divided into two types: design and manufacturing. Design problems will manifest themselves to some degree in every product where manufacturing problems are typically associated with a particular manufacturing process, parts or materials lot, or build cycle, and not necessarily appear in every product. No TMC vehicle was identified that could naturally and repeatedly reproduce large throttle opening UA effects for evaluation by the NESC team.

The combination of the VOQs distributed among a broad array of electronic components and the lack of a vehicle with a repeatable fault indicated that researching manufacturing process for a UA cause was not feasible. If a vehicle is identified with a naturally occurring UA and the UA can be repeated under controlled conditions, then researching the manufacturing of that vehicle's components would be warranted. This led the NESC team to focus on the architecture, the details of the design, and its implementation in order to determine how the system might fail, thereby creating a UA. Upon review of the architecture, the NESC team found a complex system with diverse layers of defenses against UA that balance against stranding the driver.

***F-1.** No TMC vehicle was identified that could naturally and repeatedly reproduce large throttle opening UA effects for evaluation by the NESC team.*

Due to system complexity which will be described and the many possible electronic hardware and software systems interactions, it is not realistic to attempt to "prove" that the ETCS-i cannot cause UAs. Today's vehicles are sufficiently complex that no reasonable amount of analysis or testing can prove electronics and software have no errors. Therefore, absence of proof that the ETCS-i has caused a UA does not vindicate the system. From calendar year 2005 to 2010 TMC reported approximately 11 million hours in module level software testing, and 35 million miles of system level testing. There are also many independent groups, including independent labs, hobbyists, universities, and consultants who devoted considerable time exploring potential failures.

Due to the complex nature of this problem, the NESC team applied a top-down systems engineering approach that explored the critical functions in electronic control, how the system might defend against failures and where escapes might occur. The team has extensive experience performing system engineering for complex systems of spacecraft and aircraft design and independent accident investigations that makes them uniquely suited for performing an independent assessment. The team reviewed theories from external sources and appreciated and incorporated, when possible, inputs from the NHTSA Independent Review Team. This study focused on evaluating possible failures in the MY 2005 Camry, ETCS-i that might lead to reported UA events through an exploration of the potential vulnerabilities of the design.

The NESC team had access to the design, the designer representatives, drawings, schematics, software source code, and VOQ vehicles. Data provided by TMC for review also included component and part specifications, ECM assembly and printed circuit layout drawings, details of custom application specific integrated circuits (ASICs), and details regarding the position sensors. The team also met with TMC engineers on several occasions and received additional technical information as requested. The team looked for fail-safe defenses built into the design and where these defenses might have been breached. The task presumed that a flaw existed in the electronics and used data provided by VOQs data to find out where the flaw might be, what might cause it, and how it would appear in under normal operations.

The NESC team placed their emphasis on fault detection logic, system responses to faults, and fail-safe features that were needed to protect against failures resulting in a UA. Figure 6.1-1 illustrates the flow the NESC followed in assessing potential design and implementation vulnerabilities in the TMC ETCS-i that could cause a UA. As shown in the diagram, the approach was divided into three main areas: Study VOQs and History, Testing for Understanding, and Testing for Confirmation.

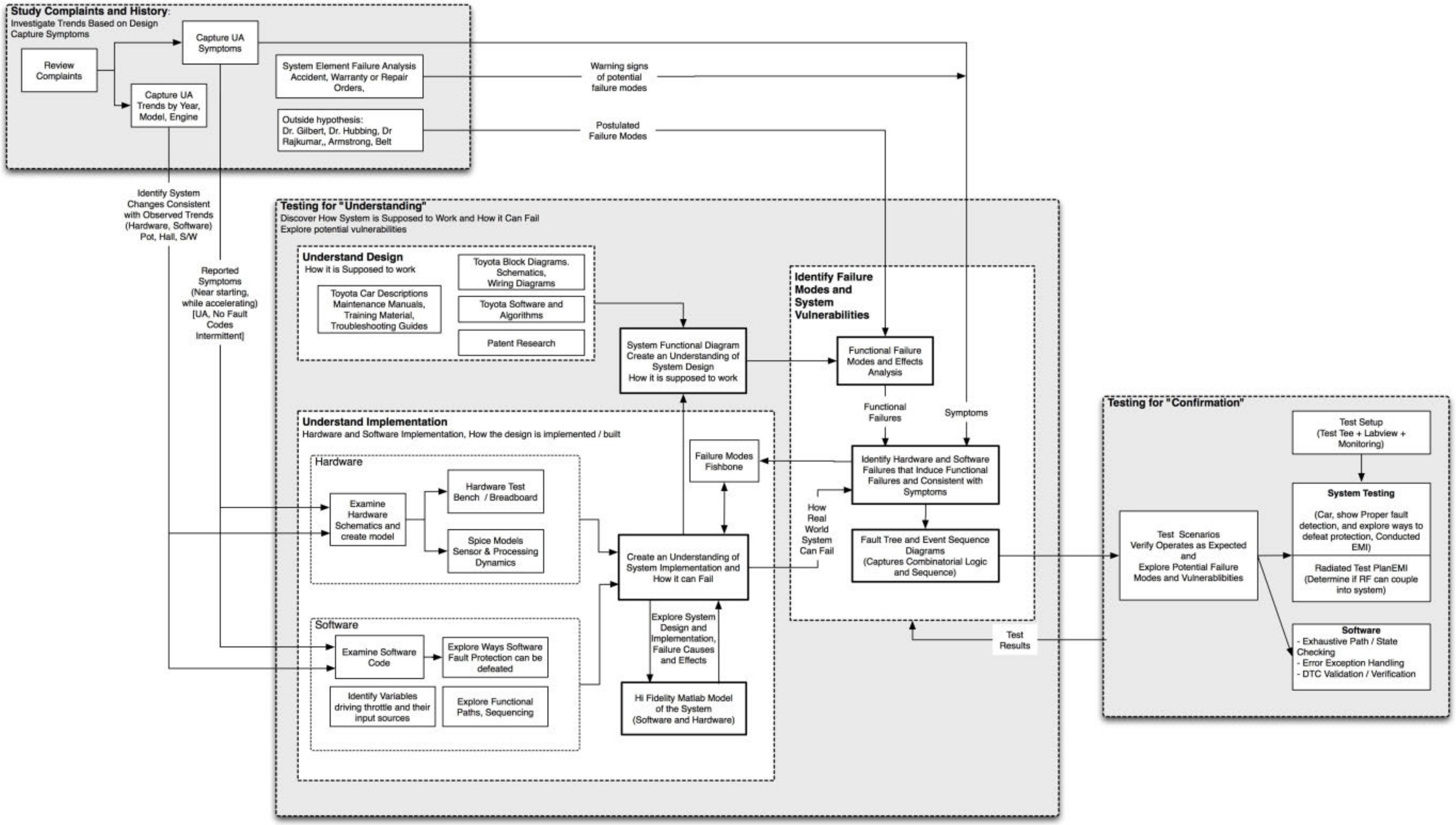

Study Complaints and History:
Investigate Trends Based on Design
Capture Symptoms
Review Complaints
Capture UA Symptoms
Capture UA Trends by Year, Model, Engine
System Element Failure Analysis Accident, Warranty or Repair Orders,
Outside hypothesis: Dr. Gilbert, Dr. Hubbing, Dr Rajkumar,, Armstrong, Belt
Warning signs of potential failure modes
Postulated Failure Modes
Identify System Changes Consistent with Observed Trends (Hardware, Software) Pot, Hall, S/W
Reported Symptoms (Near starting, while accelerating) [UA, No Fault Codes Intermittent]
Testing for "Understanding"
Discover How System is Supposed to Work and How it Can Fail
Explore potential vulnerabilities
Understand Design
How it is Supposed to work
Toyota Car Descriptions Maintenance Manuals, Training Material, Troubleshooting Guides
Toyota Block Diagrams. Schematics, Wiring Diagrams
Toyota Software and Algorithms
Patent Research
System Functional Diagram Create an Understanding of System Design How it is supposed to work
Identify Failure Modes and System Vulnerabilities
Functional Failure Modes and Effects Analysis
Functional Failures
Symptoms
Understand Implementation
Hardware and Software Implementation, How the design is implemented / built
Hardware
Examine Hardware Schematics and create model
Hardware Test Bench / Breadboard
Spice Models Sensor & Processing Dynamics
Software
Examine Software Code
Explore Ways Software Fault Protection can be defeated
Identify Variables driving throttle and their input sources
Explore Functional Paths, Sequencing
Failure Modes Fishbone
Create an Understanding of System Implementation and How it can Fail
Explore System Design and Implementation, Failure Causes and Effects
Hi Fidelity Matlab Model of the System (Software and Hardware)
Identify Hardware and Software Failures that Induce Functional Failures and Consistent with Symptoms
How Real World System Can Fail
Fault Tree and Event Sequence Diagrams (Captures Combinatorial Logic and Sequence)
Test Results
Testing for "Confirmation"
Test Setup (Test Tee + Labview + Monitoring)
System Testing
(Car, show Proper fault detection, and explore ways to defeat protection, Conducted EMI)
Radiated Test PlanEMI (Determine if RF can couple into system)
Test Scenarios Verify Operates as Expected and Explore Potential Failure Modes and Vulnerablibities
Software
- Exhaustive Path / State Checking
- Error Exception Handling
- DTC Validation / Verification

Figure 6.1-1. Assessment Approach

System and software functional diagrams were generated based on documentation and then updated from exploratory testing and from discussions with and information from TMC. Functional failure modes, fault (Ishikawa) fishbone diagrams, event sequence diagrams and fault trees were developed to assist in the analysis. Exploratory analysis and testing examined interactions of operational sequences and events along with one or multiple failure conditions. A significant amount of testing was conducted in an effort to understand how the ETCS-i operates and what fail-safes exist. Once this "testing for understanding" was completed, more formal testing of test scenarios of operational sequences, and failure conditions was completed. Appendix D contains a list of test scenarios performed in the course of this study. Multiple tests were run for each scenario with differing failure conditions on either a simulator or vehicle. For the purposes of this study, functional failures such as open circuit signal lines, short to ground, high resistance, shorts between signals, and short to source voltage and potential design vulnerabilities in fault detection and mitigation were the primary focus. Monitoring of actual responses inside the ECM hardware was not possible. However, the software model and ASIC block diagrams provided a level of insight into system function. Model responses were compared to the hardware external responses. Likewise, potential faults related to timing margins were beyond the scope of this effort. Test scenarios were conducted on a range of vehicles to encompass major changes such as the potentiometer versus Hall Effect sensor changes and ECM evolution.

In addition to exploring the ETCS-i functional failure modes and multiple failure conditions, the system was evaluated by several cross cutting disciplines, Human Factors, Electro-Magnetic Interference, and Software. Comprehensive EMC testing beyond the recommended certification levels was performed on a range of TMC vehicles to determine if exposure to EMI could result in a UA.

Human factors analyses during this study were limited to specific event sequences identified in the engineering analysis that include operator input. A review of literature on human factors as they relate to UA was performed and is discussed later in this report.

The NESC team was given the unique opportunity to review TMC source code. Independent software analysis examined the source code implementation through static analysis and the evaluation of the vehicle system software states. A functional model of the electronic control software that can drive the throttle position enabled a system-level analysis of both the vehicle hardware and software, and served as a basis for some of the hardware testing. Software analysis of the design, implementation, and execution of the MY 2005 Camry source code was performed to identify possible software faults, and software models were developed to aid in the system level analysis.

The software analysis used model-based design techniques to create high-fidelity models of the software functions and behaviors. TMC documentation and discussions with their engineering experts initiated the investigative process. Source code analysis continued the process by increasing the model accuracy. Testing on the Camry simulators and vehicles confirmed the

accuracy of the models. Efforts were made to incorporate as much actual source code into the models to further increased fidelity of the models.
This model-based design approach also supported the dissemination of the software functions and behaviors to the NESC team as a whole.

6.2 Analysis of UA VOQs

UA events have been reported, studied, tracked, and mitigations developed[5]. UA events are not unique to a manufacturer or vehicle type. Questions remain that captured the NESC team's attention:

- How often do UA events occur?
- What are the symptoms?
- Has a design change increased UA events?
- Can symptoms be traced to potential causes?

The NESC studied NHTSA VOQs. This section contains a discussion of available data on reported UA events, including their value and limitations. The NESC examined consumer VOQs to determine whether increases in the reporting of UA events coincide with design change(s). An examination of the VOQs did not identify a systematic relationship to the introduction of ETCS-i across TMC model vehicles utilizing its common ETCS-i. In addition, VOQs about the Camry were studied to classify UA event patterns to help in identifying candidate ETCS-i failure modes. A significant fraction of the Camry VOQs described events that occurred under parking and slow speed conditions where the throttle opens to a degree that driver braking attempts are reported to be ineffective. VOQs analysis also indicates some consumers have reported operating symptoms that are traceable to normal operational features of the vehicle's design

6.2.1 Sources of Information Relating to UA

First, there are many data sources that provide insight into reported UA events: voluntary reporting systems (VOQs), mandatory reporting systems (warranty claims), and accident reports (insurance companies, law enforcement, media). Each of these sources is valuable, but each

[5] Kirchhoff & Peterman, 2010; Pollard & Sussman, 1989; Schmidt, 1989.
Pollard, J And Sussman, ED (1989) An Examination of Sudden Acceleration, National highway Traffic Safety Administration, DOT-HS-807-36: DOT-TSC-BHTSA-89-1.
Reinhart, W. (1994) The effect of countermeasures to reduce the incidence of unintended acceleration incidents. National Highway Traffic and Safety Administration United States Paper (No 94 S5 0 07).
Kirchhoff, SM & Peterman, DR (22010) Unintended Acceleration in Passenger Vehicles. Congressional Research Service, R41205.
Schmidt, RA (1989). Unintended Acceleration: A Review of Human Factors Contributions. Human Factors, 31, 345-364
Sheridan, T.B. and Parasuraman, R. (2005). Human-Automation Interaction. In Reviews of Human Factors and Ergonomics, Vol. 1, pp. 89-129. Santa Monica: Human Factors and Ergonomics Society.
Stanton, N.A. and Young, M.S. (in press). A proposed psychological model of driving automation. Theoretical Issues in Ergonomic Science.
Young, M.S., Stanton, N.A., and Harris, D. (in press). Driving automation: Learning from aviation

provides different types of information, may limit which events are reported, and may be duplicated in another source.

Voluntary reporting systems include customers' complaints filed with vehicle dealer or the manufacture's customer service, and with the NHTSA VOQ system. Because the NHTSA's VOQ is the largest and most comprehensive voluntary reporting system, it will be discussed in some detail. However, many of the strengths and limitations of the VOQ will apply to the data from all such systems.

Accident reports contain a particular subset of UA events. Law enforcement databases record only those events in which a chargeable accident or moving violation occurred (i.e., in a public place and be above a certain loss value, with definitions and thresholds that vary state to state). Not all accidents with damage result in an insurance claim (i.e., parties may agree not to report to insurance). The strength of accident databases is that they often contain information that helps determine cause (e.g., detailed event description, photos, and drawings; physical evidence such as braking distance from tire marks, or condition of brakes; immediate statements from drivers, passengers, and observers; age and experience of driver; vehicle mileage; causal analyses from collision experts). However, because these databases contain only suspected UA events that resulted in accidents, it is unclear how to extrapolate from the frequency of reported UA caused accidents to the larger category of all reported UA incidents. Further, because the criteria for reporting vary from state to state, it is difficult to collate these data to obtain nationwide figures.

The Tread Act of 2000 (P.L. 106-414) mandates quarterly reporting of a variety of safety-related data, including the number of warranty claims and manufacturer field reports to NHTSA. These databases will contain only a subset of UA incidences (i.e., those that led owners to take their vehicle in for a warranty claim. Another critical limitation of these data sets is that vehicles stop contributing input once their warranty expires; thus, most warranty-claim databases offer only a three-year moving window on vehicle issues.

NHTSA VOQ

The NHTSA's VOQ is a voluntary reporting system that allows any vehicle owner to register an incident, failure, crash, or injury involving their vehicle. In addition to a free-field narrative, driver contact information is solicited, along with vehicle information (including Vehicle Identification Number which allows analysts to access missing or additional information about the vehicle's configuration).

The VOQ system shares a common approach (and therefore many of the same strengths and limitations) as NASA's Aviation Safety Reporting System (ASRS). Each of these systems provides a window into system safety by encouraging the reporting of incidents (i.e., those events that did not turn into accidents, but have the potential to be accidents). Examining the actual incident narratives was helpful when trying to identify symptoms that may correlate to potential failure modes. Specifically, VOQ information can, in principle, provide data on vehicle design deficiencies that may lead to specific events such as UA.

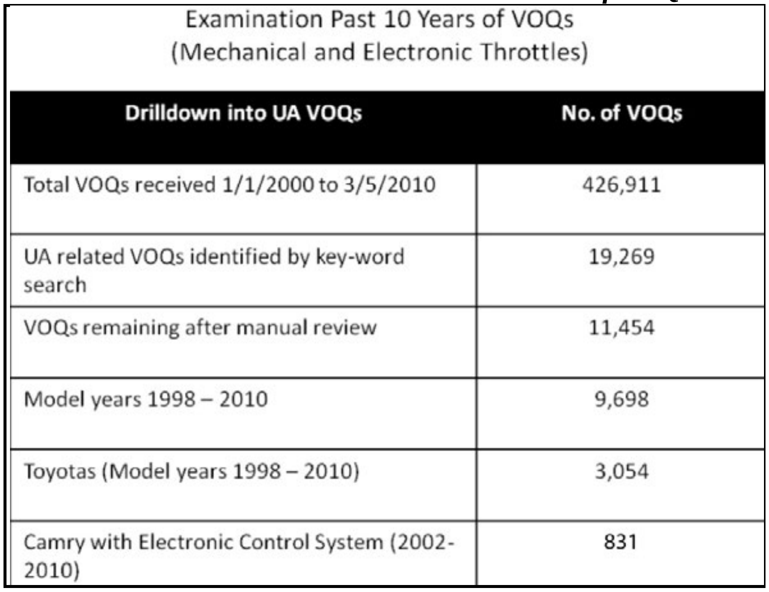
6.2.2 Characteristics of the VOQ Data

The desired “ground truth” is how often such events occur, and which precipitating factors lead to these events. The annual number of UA events across all vehicles (manufacturers/makes/ models) may be in the thousands (including both reported and unreported incidents). This sounds like a substantial number until one considers the billion of miles American drivers log every year. In truth, UA events are low-probability events best modeled as a random process.

For regulatory agencies and insurance companies, there is the additional desire to determine whether any particular vehicle model demonstrates a disproportionate likelihood of occurrence (and, ultimately, whether there is a design flaw responsible for this disparity). However, for reasons that will be discussed (and illustrated in Figure 6.2.2-1), it is extremely difficult to extract these answers from available databases.

Between January 1, 2000 and March 5, 2010, over 425,000 inputs were entered into the VOQ system (see Table 6.2.1-1). Using a keyword search[6] followed by the expert review, 11,454 VOQs were identified as being possible UA events. Of these VOQs, 3,054 involved TMC vehicles, and 831 involved Camrys with ETCS-i (i.e., MYs 2002-2010).

Table 6.2.1-1. Examination Past 10 Years of VOQs



Examination Past 10 Years of VOQs
(Mechanical and Electronic Throttles)

Drilldown into UA VOQs	No. of VOQs
Total VOQs received 1/1/2000 to 3/5/2010	426,911
UA related VOQs identified by key-word search	19,269
VOQs remaining after manual review	11,454
Model years 1998 – 2010	9,698
Toyotas (Model years 1998 – 2010)	3,054
Camry with Electronic Control System (2002-2010)	831

While the team acknowledges the strengths of the VOQ system (see Sections 6.2.4 and 6.2.5 below), a few limitations need to be discussed.

[6] Description of keyword search: The following words were used to search for possible UA events in the VOQ system: sudden, takes off, lunge, surge, accel*, unintended, unexpected, stuck pedal, pedal trapped, accelerator stuck, uncontrolled accel*, engine rev, and such.

Limitations of Voluntary Reporting Systems

The primary, intrinsic limitation of any voluntary reporting systems is that it is difficult to extrapolate from the frequency of events reported to the total number of events that occurred in the entire population[7]. While it is unlikely that reporters are fabricating events, the larger concern is that a substantial, but unquantifiable number of events go unreported.

Consider the UA event flow shown in Figure 6.2.2-1. One (or more) precipitating factors cause a UA, either low- or at-speed.

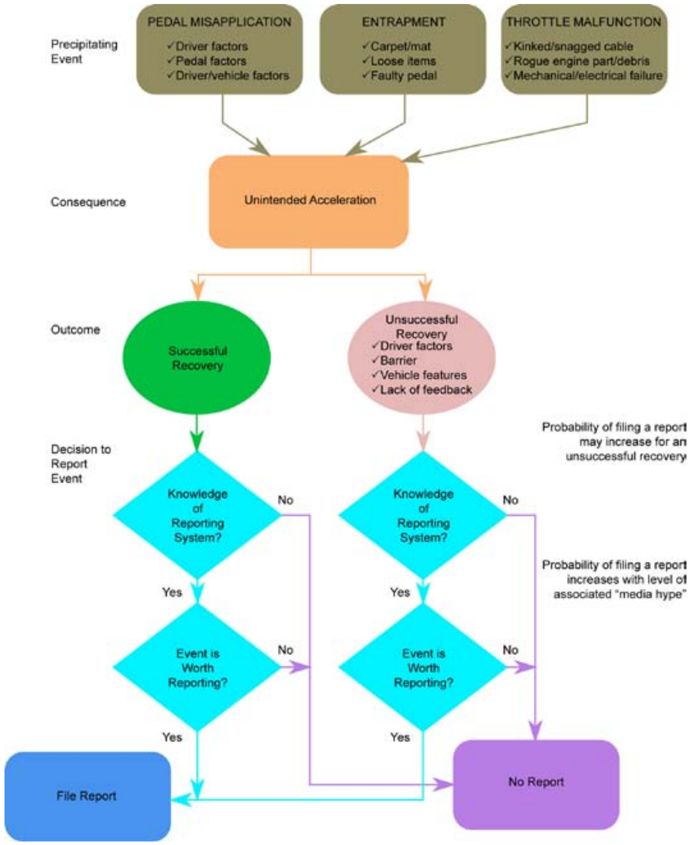


Figure 6.2.2-1.The sequence of UA events and the probabilities that such events are reported to the VOQ System

The driver can either successfully recover from the UA, or be unsuccessful in his or her recovery attempt. The NESC team posits that drivers are less likely to report a UA event if they recover successfully; thus, the probability of filing a VOQ after a successful recovery is lower than the probability of filing after an unsuccessful recovery. Note that even the probability of reporting an event after an unsuccessful recovery is almost certainly less than 1.0, given that people may

[7] Reynard, WD, Billings, CE, Cheaney, ES & Hardy, R (1986). The Development of the NASA Aviation Safety Reporting System. NASA Reference Publication 1114, pages 65-66.

not know of the VOQ system, believe the event merits reporting, or believe that such systems are not beneficial. It is possible that owners of certain vehicle types (family vehicles versus sports vehicles) or certain manufacturers have a higher or lower probability of reporting, further complicating the ability to extrapolate to the total number of events or judge whether an increase in the number of reports is related to an increase in events.

Further, both reason and report counts suggest that more VOQs are filed following media coverage of UA investigations or vehicle recalls. NHTSA received a defect petition in February, 2004, and opened an investigation, PE04-021, on March 3, 2004. The PE was publicly announced on March 7, 2004. Figure 6.2.2-2 shows the month-by-month VOQs identified as possible UAs for TMC vehicles. The marked increase in reports in 2004 coincides with the announcement (carried by Reuters and in USA Today) of the NHTSA investigation. The increases in VOQs in late 2009 and early 2010 are coincident with a TMC recall in October 2009 and publicity surrounding Congressional Hearings in early 2010.

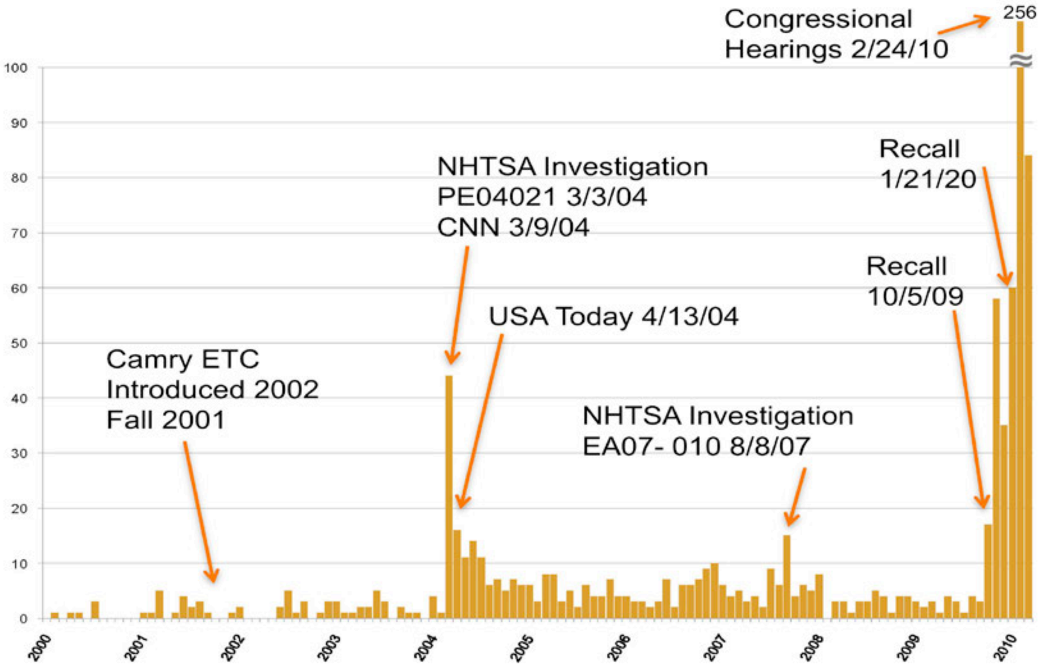


Figure 6.2.2-2. Toyota Camry VOQs Received by Month 2000-2010

It also appears that media coverage regarding TMC vehicles led to increased reporting of UA events involving other makes and models. Figure 6.2.2-3 illustrates the number of UA VOQs from all non-Toyota manufacturers for the same time period (January 2000 to February 2010).

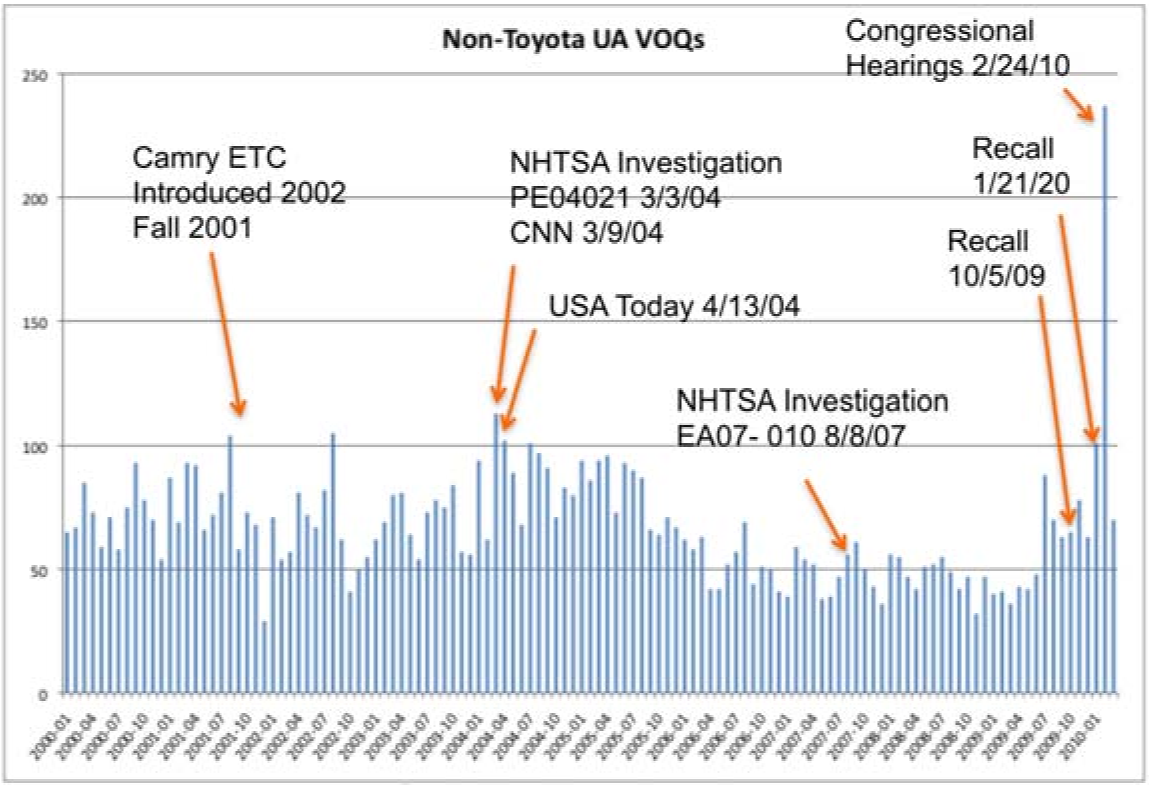


Figure 6.2.2-3. The increases in total UA VOQs for all manufacturers immediately following media attention to TMC UA-related investigations or recalls

The NESC team identified at least three reasons for such increases in reporting. First, a driver may not have been aware of the VOQ system prior to its mention in the media. Note, that even after extensive outreach campaigns, awareness of the ASRS is not 100 percent within the aviation community. Second, drivers may reconsider their non-reporting choice because they had previously dismissed the event as trivial, but now realize it may be of interest to investigators. Alternatively, drivers may choose to report an event because they anticipate an opportunity for financial gain.

However, while relative relationships among the likelihood a vehicle owner will report can be postulated, it is impossible to extract the frequencies of interest (i.e., those of the various precipitating events) from the available data.

In addition, all incident-reporting databases suffer from the limitation that the event description is provided by the driver (or an eyewitness), or for those that submit VOQs via the call in line, there is a third interpretation factor. Even when people make a sincere attempt to provide the truth their descriptions are often biased by misperceptions, memory lapses, misconceptions and inappropriate assumptions. Unless there is physical evidence for subsequent objective validation, it is impossible to determine the truth-value of the reported data.

Thus, while field report data appear to be the most logical source for evaluating whether a particular class of vehicles exhibits an unusually high rate of an undesirable driving event (e.g., UA), intrinsic flaws and limitations of these databases render such analyses inconclusive, and qualitative at best.

O-8. *The available incident reporting databases are valuable for identifying potential vehicle symptoms related to UA events. However, voluntary reporting systems may not allow for accurate quantitative estimates of incident rates or statistical trends.*

6.2.3 Relationship between VOQs and Changes in Vehicle Design

Although it has been argued that VOQs cannot be used to determine the number of UA events, the VOQ database is a source of important information. Just as with the ASRS, an increase in reports may signal a change. The change could be a combination of increased willingness to report, knowledge of the reporting system, recognition in the importance, and/or the number of events. In the past, a variety of causes have been identified and corrected to reduce UA events (e.g., the recall for floor mats).

A variety of new systems (e.g., anti-lock brakes, cruise control, electronic throttle control systems, and stability control) have been added to automobiles with a variety of consumer responses. Often introduction of new technology is concurrent with other style changes (e.g., body/window design, seat design, pedal placement, and gearshift placement). If there is a real change in the number of events, then new technology or other changes may be contributing to the occurrences.

The NESC examined consumer VOQs to determine whether increases in the reporting of UA events coincide with design change(s). Figure 6.2.3-1 illustrates the VOQs by TMC model and year. The NESC team did not observe an increase in VOQ reports coincident with the introduction of ETCS-i on all TMC models.

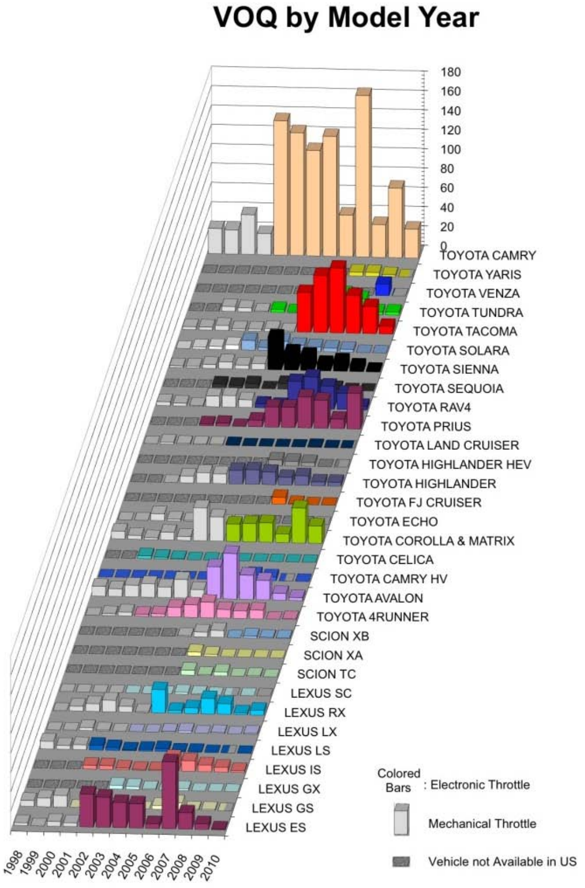


Figure 6.2.3-1. Number of VOQs by TMC Vehicle Model and MY
Grey bar indicates mechanical throttle, Colored Bar indicates ETCS-i throttle

6.2.4 Classify UA Events to Identify Candidate Failure Modes

The descriptions of the incidents in the VOQ were reviewed to assist in the identification of potential UA cause. For the purposes of consumer VOQs review, UA is any vehicle acceleration unintended by the driver. The details provided in the VOQs information on changes, such as the severity of incidents reported in VOQs has increased, repeats for a fault that was thought to have been mitigated, or a description of a new condition (hypothetically--while driving, the cruise control light came on without the operator engaging the cruise control). Hypotheses on what could be failing were generated from the narratives in the VOQs.

The NESC team reviewed all the UA VOQs submitted for the Camry, many of which included reports from interviews conducted by NHTSA with the consumers. Out of the 3054 VOQs about TMC vehicles, 959 were about the Camry model with 114 for MY 1998 to 2001 (mechanical throttles) and 831 non-hybrid Camry for MY 2002 to 2010 (ETCS-i). All of the VOQs were reviewed with the objective of exploring clues of potential failure modes. The team reviewing the VOQs consisted of six members, four from the NESC and two from NHTSA. Each of the

831 ETCS-i Camry VOQs was reviewed by at least three members. NHTSA personnel provided additional information from their customer interviews for selected VOQs. Common symptoms and event types were compared against electronics failures postulated in the failure fishbone, vulnerabilities determined from hardware and software analysis, and failures captured on the fault tree.

The VOQs were grouped (Table 6.2.4-1) based on the reviewers' assessment of the symptoms reflecting a range of causes from known vehicle operational characteristics to VOQs with unknown causes. The table includes Operational Conditions, Events and Symptoms as described in the VOQs, and Potential / Identified Causes. Where VOQ causes are unknown, electronics failure modes are identified that are traceable to postulated causes described in Section 6.5. The first three groupings reflect known causes and are described in the following paragraphs.

The first grouping shown in rows 1 through 3 with causes in light blue represents known vehicle operating characteristics. Examples include the level of acceleration cruise control utilizes going up or down hill, and the sensitivity of the accelerator pedal causing a hesitation in acceleration after the pedal is pressed.

The second grouping shown in rows 4, 5 and 6 involves acknowledged driver action. Acknowledged actions include the driver acknowledged pressing either brake and accelerator pedals, or the driver finding the accelerator pedal trapped by the floor mat. These include non-electronic generated events such as sticky accelerometer pedal, pedal entrapment by floor mats or any other items.

The third grouping shown in row 7 and colored dark blue consists of symptoms characterized by smaller acceleration caused by known features and covered by repairs orders identified by TSB. They include symptoms reflecting hesitation, delay or surging as evidenced in engine knock sensor operation, or transmission shifting and torque converter lock up.

The final four groupings address VOQ symptoms not explained by known causes. These groupings are linked to a postulated electronics causes assuming that electronics was the cause.

The fourth grouping shown in row 8 as light purple identifies surging involving a small acceleration. If electronics are postulated as the cause, it is related to throttle openings of 5 degrees above idle or less. These are manifested by lower accelerations as found with water temperature or air mass sensor anomalies.

The fifth grouping shown in row 9 as light pink is defined by mild accelerations, more than surging, but less than hard to control acceleration. If these were caused by the electronic throttle they would be commensurate with relative throttle openings between 5 and 25 degrees above idle, such as the acceleration from the cruise control system at higher speeds.

The sixth grouping shown in rows 10, 11, and 12 as red is characterized by accelerations that are hard to control and in many cases the VOQs indicate that that driver brake application did not control them. If the electronic throttle were to cause these high accelerations, they would be characterized by throttle openings greater than 25 degrees above idle. The selection of 25 degrees to characterize high acceleration is described in 6.4.2. This group's characteristics include high accelerations from low speed or parking where the brakes may not be effective, high engine speed and difficulty holding the vehicle stationary with the brakes, or sustained high power acceleration beyond the driver command or after the driver has released the accelerator pedal.

The final group shown in row 13 and colored white is for those VOQs that could not be placed into rows 1 through 12 because of insufficient information.

Detailed review of the Camry VOQs and the sampling of other TMC models suggest that some drivers may not know or understand the vehicle's response to hazard controls.

Table 6.2.4-1. VOQ Binning

Row	Operational Conditions	Events and Symptoms	Potential / Identified Causes
1	While Starting /Stopping and at Lower Vehicle Speeds	• Accelerator Pedal is too sensitive as identified by the driver. Vehicle lurches forward as pedal is pressed. • Fast idle influencing driving, warm engine. Engine speed slow to go back to idle (1 to 2 second delay in closing of the throttle valve at slower speeds). • Loss of engine braking when the throttle is released. • Engine speed increase when air conditioning activates/cycles. • Fast idle influencing driving, cold engine or after engine restart and before engaging gear. Engine speed remained high during warm-up/restart.	• That is the way the pedal gains are designed, too sensitive for some • That is the way vehicle works, higher engine speed held a little before going back to idle • Normal idle speed operation • That is the way vehicle works, higher engine speed required during engine warm-up to prevent engine stall.
2	Braking and Braking Over Certain Road Surfaces	• Vehicle braking (deceleration) reduces when braking over bumps, or loose/low friction road surface.	• Identified/suspected ABS activating
3	During or Related to Cruise Control Operation	• Cruise control doesn't control vehicle speed on downhill slope. • Cruise control accelerates beyond set point by a few mph. • Cruise control accelerates/causes high engine speed when going uphill. • Cruise accelerates too fast/aggressive when re-enabled/resumed. • Cruise control accelerates too fast when approaching traffic.	• Cruise control not intended to control on downhill slope • Vehicle can overshoot a little, the way vehicle works • When cruise control seeks the set speed it will do so at .06 g and use throttle; the transmission will downshift if needed • Cruise control accelerates at .06 g, does down shift, high engine speed • Driver perception
4	Highway Merging, Passing, Accelerating at Road Speed	• Floor mat trapped pedal. Acknowledge by driver.	• Driver/NHTSA identified floor mat trapped pedal.
5	Braking and Braking Over Certain Road Surfaces	Delayed braking, or ABS activation	• Delayed braking
6	While Starting /Stopping and at Lower Vehicle Speeds	• Driver acknowledged dual accelerator and brake pedal application • Accelerator Pedal Stuck and was cleared by driver	• Driver acknowledged dual pedal application • Driver acknowledged pedal stuck and cleared. Could also be floor mat restraining pedal

Row	Operational Conditions	Events and Symptoms	Potential / Identified Causes
7	Driving at Roadway Speeds	• Surging while shifting, ~40 mph (35 - 45 mph range). Hesitation, delay and surging while accelerating but not related to transmission activity. May be related to operator application of pedal (delayed/lagging engine output and subsequent over-output).	• Identified torque converter lock up design feature, <5 degrees Throttle • Known hesitation and engine knock sensor transmission shifting issue fixed by TSB, <5 degrees Throttle
8	Driving at Roadway Speeds	• Surging while driving, at constant accelerator pedal application.	. • If electronics <5 degrees Throttle, A/F sensor failures, water temperature or throttle works that way.
9	During or Related to Cruise Control Operation	• Cruise control accelerates beyond set point by more than a few MPH.	• If electronics , >5 degrees Dual Lane Failure or Software Malfunction • If electronics ,failure in combination meter resulted in low speed reading and acceleration
10	While Starting /Stopping and at Lower Vehicle Speeds	• Low speed or parking, sometimes initiated by braking. Involves high power level, brake application doesn't stop/slow vehicle or is ambiguous. • Low speed or parking initiated by accelerator application, brake application doesn't stop the car. • Engine speed increases when/while accelerator is applied, brakes reportedly effective. • Driver states high engine power while foot is on the brake, vehicle remains stationary or is highly restrained, and brakes are fighting the acceleration/engine power output.	• If electronics would be the cause, >35° Throttle Opening, • If electronics it has to fail within the tolerance, be a dual failure, or a software failure without any indication
11	Driving at Roadway Speeds	• Large increase in engine power output (near full power) coincident with brake pedal application possibly in response to an unexpected event/emergency. • Sustained high power acceleration in excess of the driver's accelerator pedal application, and/or after the driver has released the accelerator pedal.	• If electronics would be the cause, >25 degrees Throttle Opening above idle • If electronics, it has to fail in the allowable lane, dual failure, or software leaves no DTC
12	Highway Merging, Passing, Accelerating at Road Speed	• Vehicle accelerates on highway after passing, or after merging into traffic (i.e., after accelerator application).	• If electronics would be the cause, >25 degrees Throttle Opening above idle • If electronics, it has to fail in the allowable lane, dual failure, or software leaves no DTC
13	Unknown	Unknown cannot understand the VOQ.	Requires more information.

Color Keys

Vehicle Feature	UA Surging, Small Acceleration <5 degrees Throttle Increase
Driver Acknowledged	UA Medium Acceleration, Effective Braking, >5 and <25 degrees Throttle Increase above idle
Vehicle Technical Service Bulletin	UA Large Acceleration, Degraded Braking, >25 degrees Throttle Increase above idle

The outcome of the VOQ analysis is shown in the Figure 6.2.4-1. VOQs with known causes are shown in the three groupings with the blue tints traceable back to Table 6.2.4-1 rows 1-7. These include the known vehicle operational features, driver acknowledged causes, and known items covered by TSBs. The three VOQ groupings of with unknown causes are tinted red representing three ranges of throttle openings if the electronics were the cause. These postulated electronics causes involve: less than 5 degrees; greater than 5 degrees, but less than 25 degrees; and greater than 25 degrees throttle openings above idle.

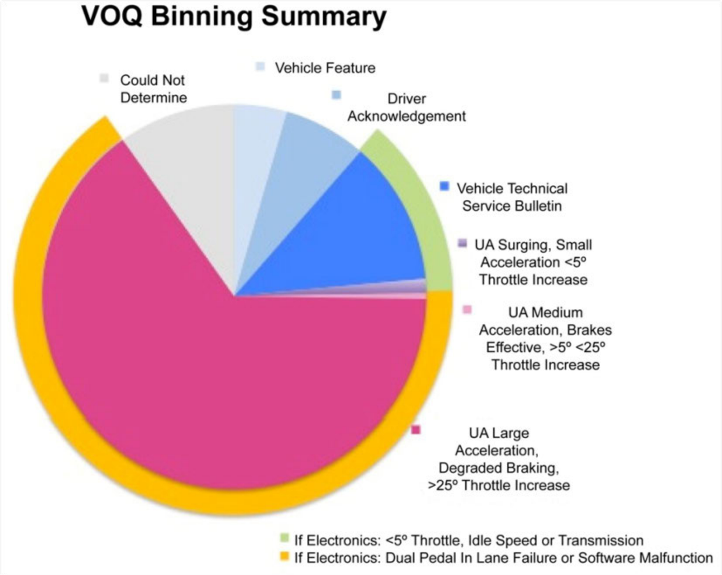


Figure 6.2.4-1. VOQs Binning by Major Group

The majority of reported VOQs had an unknown cause and fall within the yellow arc. They are characterized by postulated UA large acceleration with a >25 degree-throttle increase above idle. To create a condition matching these reported VOQs, failures need to mimic valid accelerator pedal signals or involve a software malfunction. 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, as described in Section 6.6.2. Software malfunctions would need to unilaterally create a large throttle command as described in Section 6.7.

The next largest set of reported VOQs fall within the green arc, are associated with postulated low accelerations (i.e. less than 5 degrees throttle increase). They include the known Vehicle TSBs, Vehicle features and UA Surging. In addition, a small fraction of reported VOQs with unknown causes, shown in the pink section, if caused by electronics, include functional failures of idle speed control (ISC), transmission control, Vehicle Stability Control (VSC), and throttle assembly. These postulated failures may result in throttle opening less than 5 degrees as described in Sections 6.5 and 6.6. Known TSB items such as engine knock sensor and transmission shifting issues are also at the low acceleration level.

The rest of the reported VOQs fall in to either the unknown category shown in white, or a known vehicle feature, or driver acknowledged action.

Examining the 540 VOQs with postulated >25 degree relative throttle opening and degraded or anomalous braking shows a preference in reported UA incidents occurring early in the vehicle's life with the largest number in the first 10,000 miles. Figure 6.2.4-2 for MY 2002 to 2006 potentiometer accelerator sensor vehicles shows a decreasing trend starting at the beginning of life and then leveling off after 60,000 miles. Vehicles with Hall Effect accelerator pedal sensors show a similar overall trend as shown in Figure 6.2.4-3.

Postulating these UA incidents are the result of a single electronics failure would imply some kind of infant mortality failure as opposed to failure causes related to exposure after delivering a properly functioning vehicle.

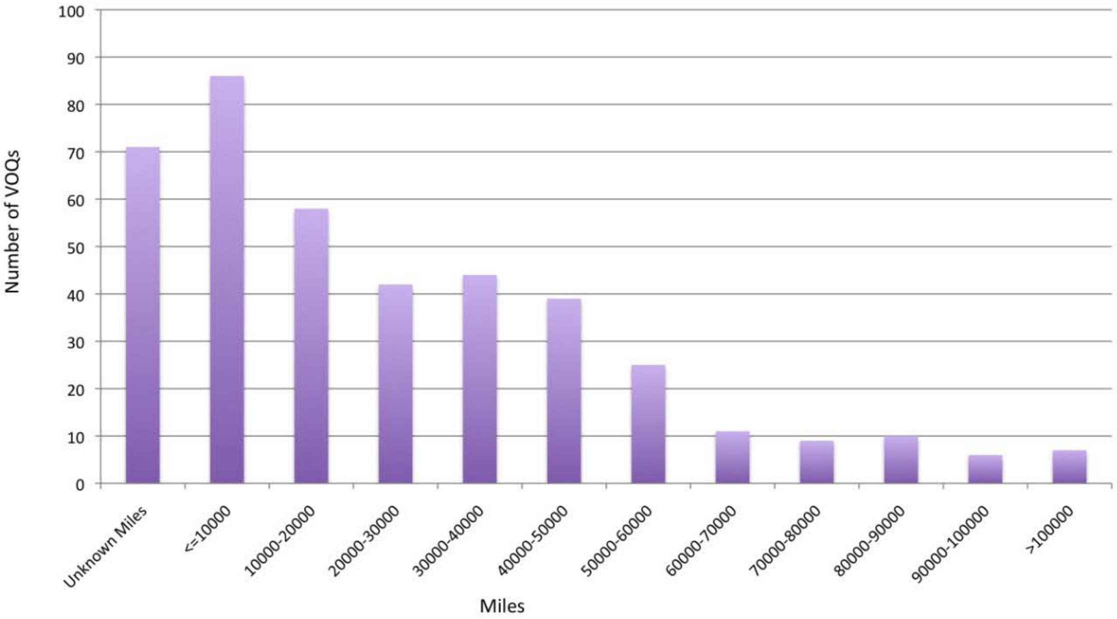


Figure 6.2.4-2. 408 Camry VOQs for MY 2002-2006 with Potentiometer Accelerator Sensor with >25° Relative Throttle Opening and Degraded or Ambigous Braking by Incident Mileage

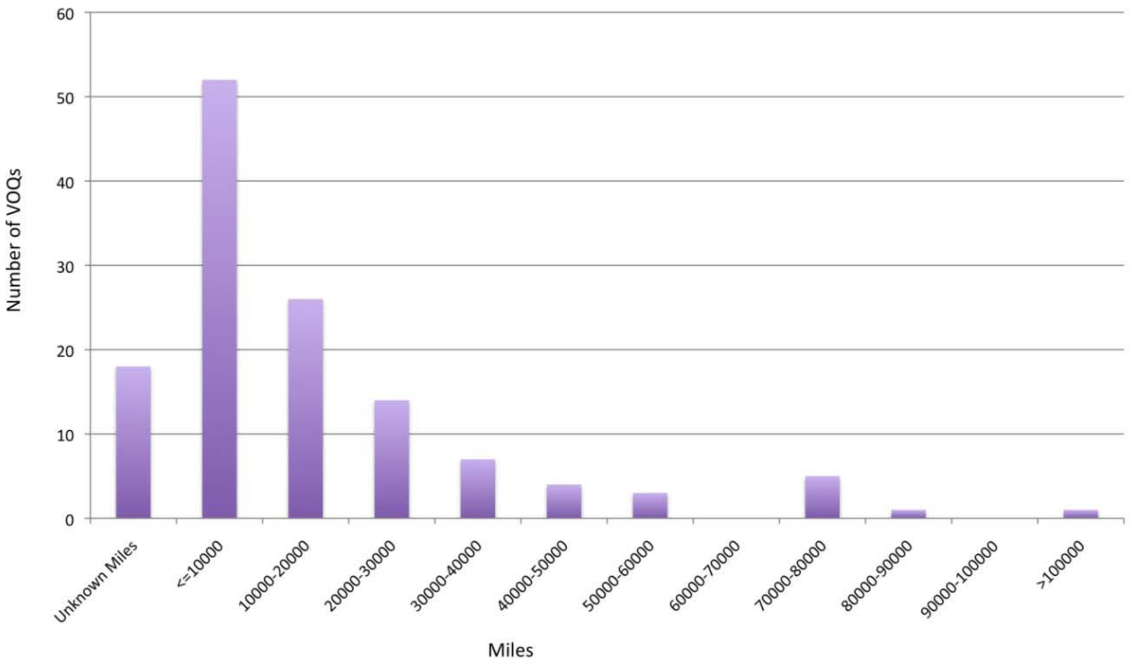


Figure 6.2.4-3. 131 Camry VOQs for MY 2007-2010 with Hall Accelerator Sensor with >25 degrees Relative Throttle Opening and Degraded or Ambiguous Braking by Incident Mileage

6.2.5 Warranty Data

Warranty repair records can provide data indicating whether electronics failures occur in large enough quantities to corroborate an electronics cause of UAs. A dual failure is postulated to cause a condition that can result in unintended larger than >25 degrees relative throttle openings as described in 6.5.2. This postulated condition would require two single failures therefore warranty records should contain a higher incidence of these single failures.

Review of VOQs and warranty data during the first 36,000 miles involving accelerator pedal circuits indicates there are fewer reported warranty repairs than reported UA incidents consistent with large postulated >25 degrees relative throttle openings with degraded braking.

VOQ analysis described in Section 6.2.4 indicates a total of 540 VOQs might be caused by electronics if the failures result in large throttle openings greater than 25 degrees above idle. Figure 6.2.5-1 shows most of these reported incidents, with mileage noted, 132 occurred in the first 10,000 miles of vehicle operation with 305 occurring within a nominal 36,000 warranty period. Of the 404 accelerator pedal warranty returns, 249 occurred within the first 36,000 miles.

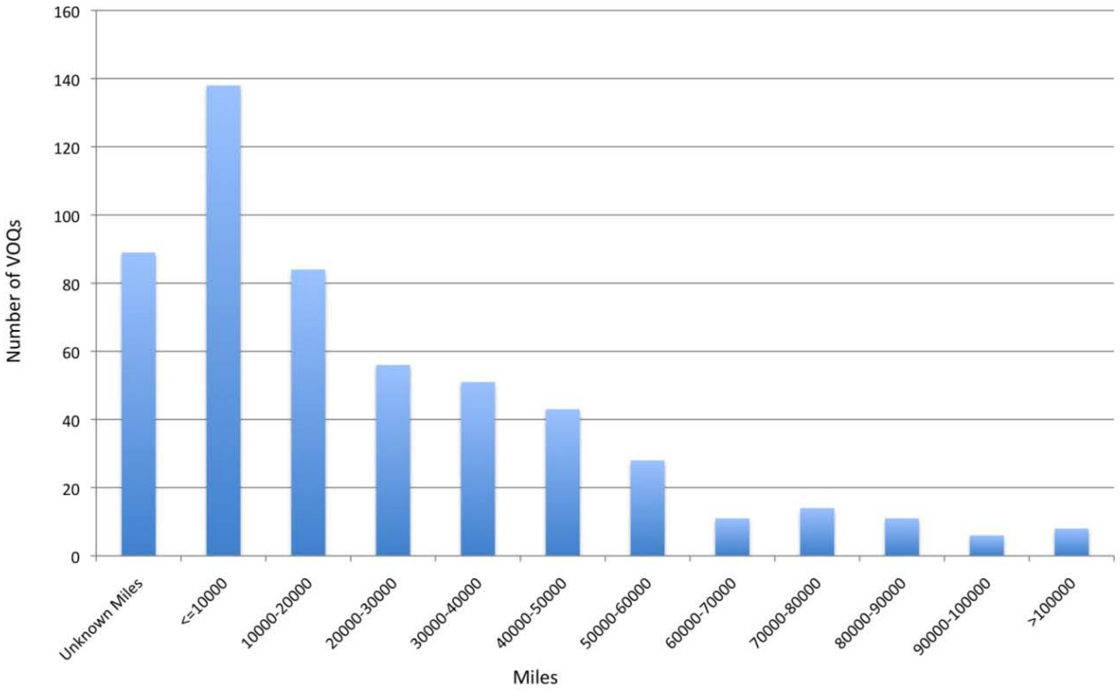


Figure 6.2.5-1. Camry VOQs by Incident Mileage
Of the 539[8] VOQs describing large acceleration with degraded braking, most occur in the first 10,000 miles of vehicle operation with 305 reported within a nominal 36,000 mile warranty period.

The NESC team reviewed the warranty repair data provided by TMC to NHTSA. Of a total of approximately 429,000 repair items roughly 24,000 apply to the Camry. Initial examination focused on identifying trends of high volume repairs involving electronic throttle components such as the throttle body, the ECM, and the accelerator pedal assemblies. Initial examinations did not identify high volume ETCS-i repairs for the 3.4 million vehicles in the total Camry data set.

Detailed examination of Camry warranty repair items centered around DTCs and repair items involving the accelerator pedal circuits because system analysis and testing indicated a postulated cause of >35 degrees (absolute) throttle increase (>25 degrees relative) UA involved dual accelerator pedal sensor failures and/or their interface electronics to the ECM.

It was postulated that evidence of dual failures might be occurring if repair data shows a large number of single failures or near misses.

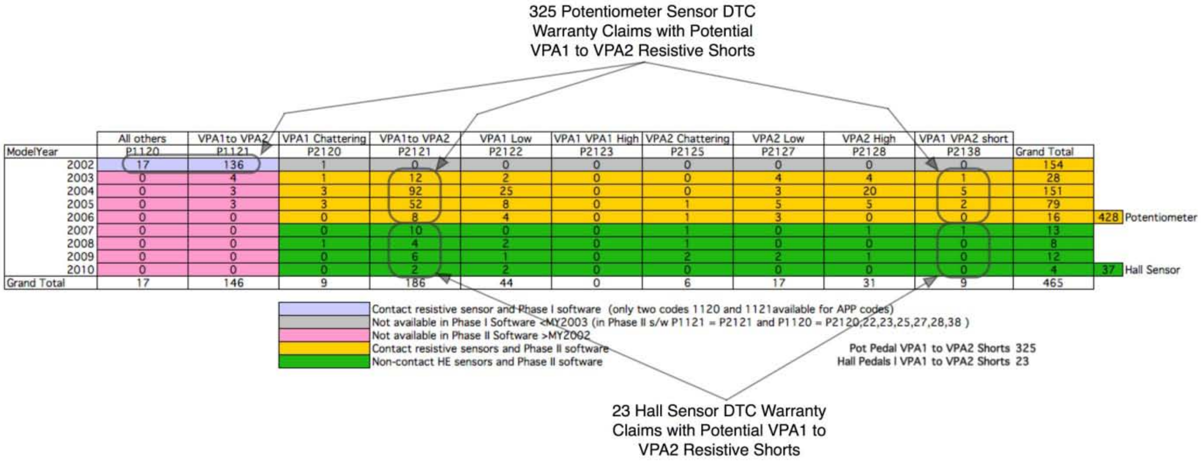
Of the roughly 24,000 Camry repair items, 465 accelerator pedal DTCs were flagged on 404 repair cases. There were 61 cases involving multiple DTC in a repair case.

[8] One VOQ did not indicate vehicle MY.

The 404 repair cases were further separated by Camry vehicle MY, DTC and the pedal potentiometer and Hall sensor types. DTC 2121 for MY >2002 and DTC 1121 for MY 2002 includes resistive connections between VPA1 and VPA2, or a resistive connection of either VPA to power or ground, necessary ingredients for one of the dual pedal sensor failures. DTC 2121 could also be caused by either failures resulting in the VPA1 and VPA2 signal pair not in the operational lane as further described in Section 6.6. There were a total of 348 flagged DTCs presented for warranty repair for VPA1 and VPA2 signal pair not in the operational lane, as described Section 6.6.2, potentially caused by a resistive short.

Table 6.2.5-1 indicates that of these warranty repairs there were a total of 325 anomalies for the potentiometer sensor vehicles and 23 anomalies for Hall Effect sensor vehicles.

Table 6.2.5-1. Accelerator Pedal Warranty Repair Counts



325 Potentiometer Sensor DTC Warranty Claims with Potential VPA1 to VPA2 Resistive Shorts

	All others	VPA1to VPA2	VPA1 Chattering	VPA1to VPA2	VPA1 Low	VPA1 VPA1 High	VPA2 Chattering	VPA2 Low	VPA2 High	VPA1 VPA2 short		
ModelYear	P1120	P1121	P2120	P2121	P2122	P2123	P2125	P2127	P2128	P2138	Grand Total	
2002	17	136	1	0	0	0	0	0	0	0	154	
2003	0	4	1	12	2	0	0	4	4	1	28	
2004	0	3	3	92	25	0	0	3	20	5	151	
2005	0	3	3	52	8	0	1	5	5	2	79	
2006	0	0	0	8	4	0	1	3	0	0	16	428 Potentiometer
2007	0	0	0	10	0	0	1	0	1	1	13	
2008	0	0	1	4	2	0	1	0	0	0	8	
2009	0	0	0	6	1	0	2	2	1	0	12	
2010	0	0	0	2	2	0	0	0	0	0	4	37 Hall Sensor
Grand Total	17	146	9	186	44	0	6	17	31	9	465	

🟪 Contact resistive sensor and Phase I software (only two codes 1120 and 1121available for APP codes)
⬜ Not available in Phase I Software <MY2003 (in Phase II s/w P1121 = P2121 and P1120 = P2120,22,23,25,27,28,38)
🟥 Not available in Phase II Software >MY2002
🟨 Contact resistive sensors and Phase II software
🟩 Non-contact HE sensors and Phase II software

Pot Pedal VPA1 to VPA2 Shorts 325
Hall Pedals I VPA1 to VPA2 Shorts 23

23 Hall Sensor DTC Warranty Claims with Potential VPA1 to VPA2 Resistive Shorts

Figure 6.2.5-2 plots the DTCs versus MY showing each MY's contribution to the total repair counts. Potentiometer equipped vehicles represent a larger percentage of the total number of 2121 (1121) DTC with declining trends from 2002 through 2006. Hall Effect sensor equipped vehicles from 2007 to 2010 also show low warranty repair rates.

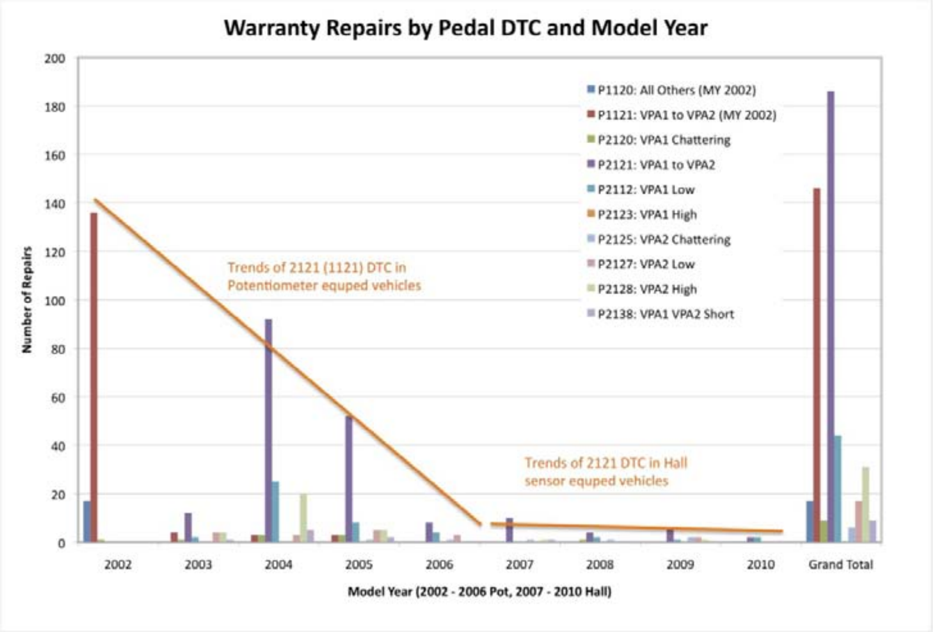


Figure 6.2.5-2. Warranty Repairs by Pedal DTC and Model Year

Potentiometer sensor accelerator pedal DTC 1121 and 2121 repair mileages indicate an increasing trend over time throughout the 36,000 mile warranty period, Figure 6.2.5-3. Between 30,000 and 40,000 miles the repair rate starts to drop and it is not clear the rate reduces due to sensor performance or the standard warranty expiration.

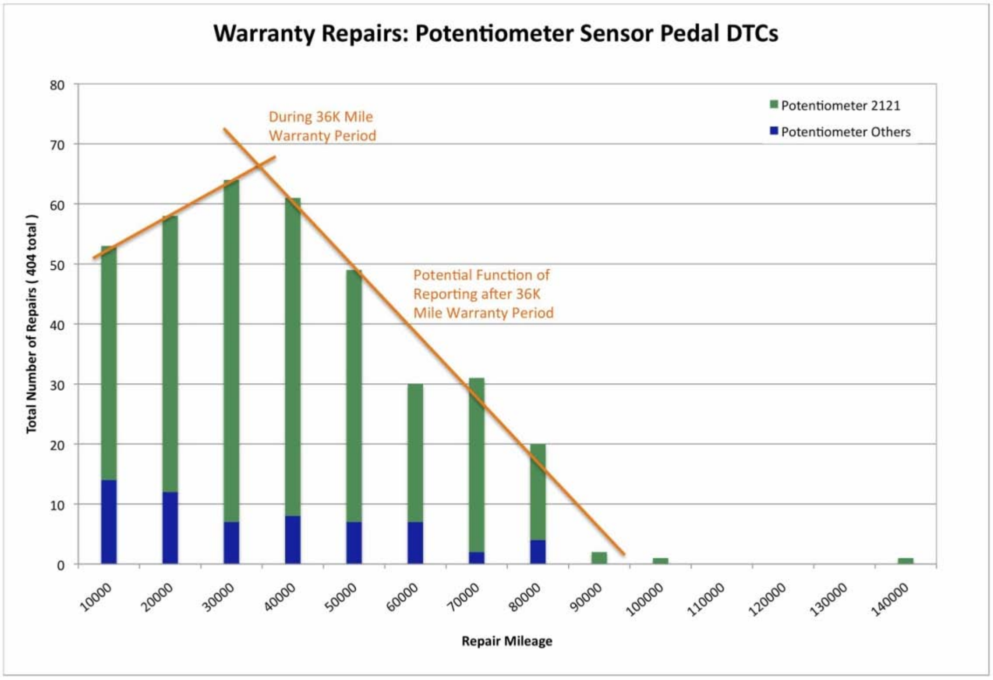


Figure 6.2.5-3. Potentiometer Sensor Pedal DTCs

Hall Effect sensor accelerator pedal DTC 2121 repair mileages indicate a relatively constant trend over time throughout the 36,000 mile warranty period, Figure 6.2.5-4. Between 30,000 and 40000 miles the repair rate also drops and it is not clear whether the rate reduces due to sensor performance or the standard warranty expiration.

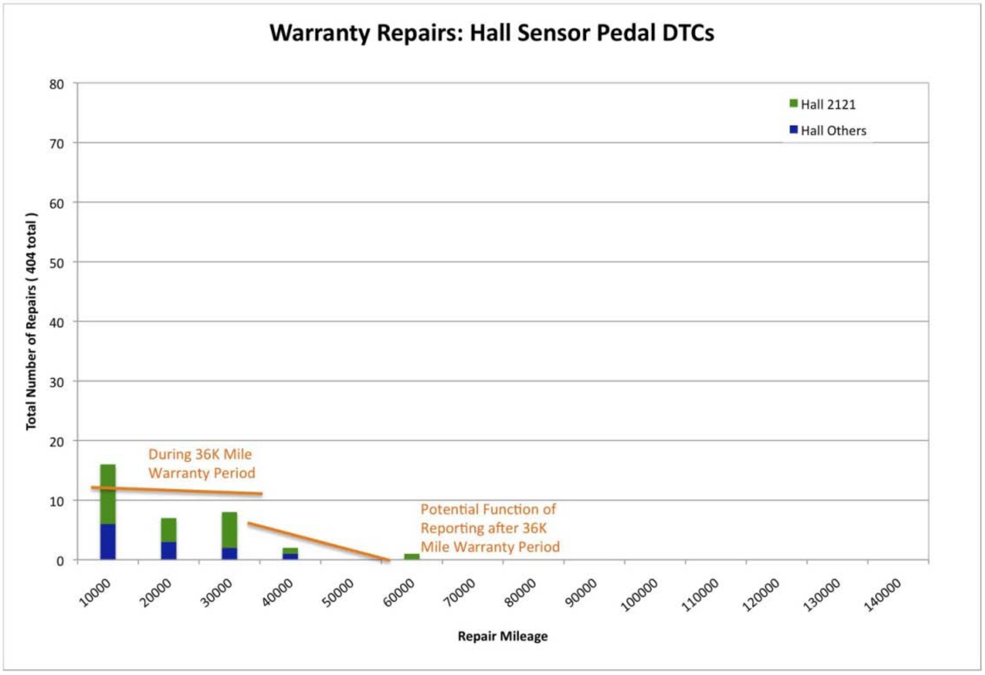


Figure 6.2.5-4. Hall Sensor Pedal DTCs

6.3 Human Factors on UA Events and Current Trends in Automotive Technologies

The current investigation illuminated a number of Human Factors (HF) issues. Several of these issues may impact the frequency of UA events and the likelihood that they are reported. More critically, all five of these issues may have broader implications for the safe and successful integration of driver and vehicle, impacting not only the likelihood of driver error, but also the driver's ability to recognize and recover from emergency situations. These five HF issues are:

1. Standardization versus brand identity.
2. Reduction of perceptual feedback to the driver.
3. Unintended consequences of design decisions.
4. Migration toward shared control authority.
5. Challenges of studying HF contributions to UA events in the laboratory.

6.3.1 Standardization versus Brand Identity

One might think this conflict could be reconciled by agreeing to standardize the design of critical controls and safety features. For example: The accelerator pedal is always to the right of the brake pedal. But, could it be standardized how far to the right? How much closer to the floor? Whether the brake pedal is to the left or right of the steering wheel centerline? The driver's seat center line?

New safety features often start out as high-end options (or on high-end vehicles), then migrate over time into standard equipment. As airbags took this path, there were lessons learned regarding integration into a general fleet filled with small children and babies in car seats. Tire-pressure monitors have recently become standard equipment, yet 46 percent of drivers still cannot interpret their warning symbol[9]. Antilock brakes are a safety feature, but they still are not standard equipment. Knowing whether your vehicle is equipped with them is critical in executing the correct emergency braking response, yet few drivers consult the instrument panel lights to determine whether an unfamiliar vehicle is equipped with them.

Drivers should also attend to their “Check Engine” light. If it comes on while one is driving, it means…something. What that something is depends on the vehicle’s make and MY. Introduced in the 1980s as the driver’s “window” into the vehicle’s onboard diagnostics (OBD) system, the light initially was used to indicate a malfunction in a monitored vehicle performance parameter (e.g., fuel mixture, ignition timing). The actual nature of the malfunction was encoded in the OBD CPU, to be accessed by a service technician. Starting in 1996, OBD II regulations required that systems monitor a myriad of emission control parameters. In the words of John Van Gilder, General Motor’s lead OBD development engineer, “The ‘Check Engine’ light is reserved only for powertrain problems that could have an impact on emissions systems”[10] (at least on GM vehicles). On the MY 2002 Mazda Protégé, it could be an electrical problem. On the MY 2007 TMC Matrix, it could be a transmission problem. Generally, a red light indicates a more severe problem than an amber light, and a flashing light indicates greater severity than a steady light. One should consult, for specifics, the owner’s manual; however, this may not be available in the glove box.

The primary concern of the Check Engine Light (and, in fact, the entire OBD system) is to convey information about “vehicle health” – that is, how well the vehicle, or at least its emissions system, is functioning. At best, it provides only an indirect indication of whether or not the vehicle is safe to drive. That function is left to other indicators, such as the tire pressure warning light.

There is a new generation of “smart” safety features vehicle manufacturers are introducing that will be discussed in more detail in Section 6.3.4. These systems will warn drivers before drifting out of their lane, changing lanes if another vehicle is there, closing too quickly on the vehicle ahead of them, or performing other unsafe driving maneuvers. As was the case for airbags and ABS, these features will most likely initially be offered as high-end options (or standard equipment on high-end vehicles), with migration to lower-cost makes and models over the following decade. Drivers may not always know whether the vehicles they are driving are equipped with these features. Further, given the proprietary nature of these technologies, the

[9] *According to a survey conducted by Schrader, a company that makes tire-pressure monitoring systems. Cited in http //autos.yahoo.com/articles/autos_content_landing_pages/1498/do-you-know-what-this-symbol-means*

[10] *Quoted in ConsumerReports.org’s “What to do if the check engine’ light goes on.” Available at http //www.consumerreports.org/cro/cars/new-cars/news/2005/what-to-do-if-the-check-engine-light-goes-on/overview/index.htm*

“same” system (e.g., “safe following”) may behave differently on different vehicles. If the vehicle being driven behaves in an unexpected manner, the driver may be unable to determine whether the vehicle is malfunctioning or simply exhibiting an unexpected “smart” feature.

When one twists a column stick on a rental vehicle and turns on the windshield wipers instead of the lights, it’s an annoyance. If one pumps the vehicle’s ABS in a panic stop, or can’t locate the parking brake, or doesn’t understand the vehicle’s “behavior”, then the result may prove far more severe.

6.3.2 Reduction of Perceptual Feedback to the Driver

Drivers use perceptual feedback to monitor the state of their vehicle and the efficacy of their control inputs. However, design trends over the past several decades have led to reduced environmental feedback (e.g., suppressed road and engine noises), reduced cueing from control devices, and reduced or altered linkages between driver inputs and vehicle responses. In concert, these loosen the link between the vehicle and the driver that is critical for safe driving. As an example, consider the design of the primary floor pedals: the accelerator and brake.

In the case of UA events, great attention has been focused on pedal misapplication as a possible cause. Pedal misapplication occurs when the driver erroneously applies the accelerator and mistakes it for the brake, or inadvertently applies both. The placement of acceleration and brake pedals was mentioned above, both in relation to each other and to other reference points of the vehicle, and varies among makes and models. This means the driver cannot depend on a consistent kinesthetic location cue to differentiate the two pedals between vehicle makes and models. But there are other design factors that impact the pedals’ ability to be discriminated.

In addition to the pedals’ statics (i.e., their positions in three-dimensional space), there are also the kinematics (i.e., is the motion constrained by a top hinge or a bottom hinge) and dynamics (i.e., how much force is needed to move the pedal, and how the required force varies over the course of the pedal’s motion arc). Additionally, there is tactile feedback from the pedal. This can be subtle given the barrier of shoes, but drivers can often differentiate vertical and horizontal pedal pad grips. Next, there is the vehicle’s response to the pedal input. If the driver accidentally presses on the accelerator pedal, the consequence should be an immediate revving of the engine. If that sound (noise) is damped (or lost in the sound/noise of a six-speaker stereo system), or if the vehicle’s response is delayed because the command is “vetted” through the vehicle’s control system, then the driver is less likely to realize an error.

In isolation, each of these design decisions may seem benign or even positive: bottom-hinged pedals may be less prone to carpet/mat entrapment; matching pedal pads may be more stylish; who doesn’t want less engine noise? But, in concert, these choices mute the driver’s perceptual experiences, which, in turn, can compromise safety. This leads to the issue discussed in Section 6.3.3.

6.3.3 Unintended Consequences of Design Decisions

This issue was mentioned with regards to top-hinged accelerator pedals; here, the designer is striving to minimize one potential problem (mat entrapment) without realizing a new problem is created (reducing a kinematic cue that differentiate the accelerator and brake pedals). Even more striking are cases where a design is selected to minimize the likelihood of one driver error while inadvertently introducing (or increasing the likelihood of) another driver error.

In some cases of UA in TMC vehicles (including Lexus), the drivers reported that they could not recover from the UA because they were unable to shift into neutral or turn off the vehicle. Upon investigation, it was noted that such difficulties were encountered on vehicles with sport shifters and keyless ignitions.

Sport shifters were introduced to give drivers of automatic transmissions a sense that they can still control their vehicles' drive gear. Rather than bother with a clutch and manual floor shift mechanism, one pushes the automatics' shifter toward the "+" sign to up-shift, or toward the "-"sign to downshift. To prevent the driver from inadvertently shifting into neutral while trying to up-shift, the +/- shift channel is displaced from the normal P-R-N-D channel, for Toyota, it is typically toward the driver.

Unfortunately, due to the parallel shift channels, the labels for "+" and "N" are often proximal. Moreover, when the driver grabs for the shifter in an emergency such as a UA, the driver could jam the control into the +/- channel. It is then quite easy to make the preservative error of pushing the shifter toward "+" in an attempt to reach "N". Thus, the separate-channel design, which safeguards against an inadvertent shift into neutral, can precipitate the error of being unable to "find" neutral in an emergency UA situation.

The keyless (push-button) ignition design can likewise have an unintended consequence. Here, the concern was that the driver (or passenger) might inadvertently turn off the vehicle when it is in motion. To prevent such an error, the safeguard was added that the button must be held for three seconds to turn off the vehicle when the vehicle is in motion. However, this procedure is certainly not well practiced by drivers. Indeed, many owners are not even aware of this "hold the button" requirement. In any case, the most common behavior in an emergency situation is to revert to the well-learned, oft-practiced, always-successful procedure: push the button briefly to turn off the vehicle. However, this procedure fails in this off-nominal situation, no matter how many times the driver executes it in rapid succession.

Care must be taken, then, to ensure that the design solution to one problem does not become the cause for another. Thus, while there is testimonial evidence that pedal misapplication is one cause of UA, any re-design effort to reduce the ability to confuse the two pedals must be vetted to ensure that other aspects of braking performance (e.g., the time to transition from the accelerator to brake pedal) are not negatively impacted.

6.3.4 Migration Toward Shared Control Authority

As automotive technology advances, designers reach an application transition point that may seem trivial from a technological perspective, but which has profound HF application: the introduction of “smart” technologies that are given the authority to over-ride (or limit) driver inputs.

From a technological standpoint, it can be a relatively trivial difference whether the onboard system that tracks range and range-rate uses the result to issue an auditory warning or to decelerate the vehicle. From the standpoint of control authority, this difference is huge. In the first case, the onboard system acts in an Advisory Capacity; that is, its role is limited to advising the driver of a potentially hazardous situation. In the second case, the system is given the Control Authority to alter the vehicle state directly without direction or approval from the driver (Sheridan & Parasuraman, 2005).

As was learned from other domains of complex system control (e.g., aviation, power plants), such a Shared Control Authority mode could lead to human error (Young, Stanton, & Harris, in press). The operator may become confused about the system state, the automation’s “intention,” and even “who” is currently in charge. Human and automation can end up working at cross-purposes, with the operator “fighting” the automation or relinquishing responsibility to a system that has “developed its own agenda.” Issues with Shared Control Authority have occurred with highly trained operators, controlling systems where time-critical decisions typically unfold over minutes (or even hours).

It is suggested that the American driving public is not a prime target population for Shared Control Authority operations (Stanton & Young, in press). Driver’s training (especially for off-nominal and emergency situations) is minimal; they transition among systems (cars) with little awareness of that particular system’s technologies and capabilities. Further, many drivers consistently demonstrate a cavalier attitude regarding both the potential damage these systems can inflict and their responsibility to maintain vigilance and safe operating envelopes.

Many designers would use these same operator characteristics to argue for the implementation of “smart” systems to compensate for drivers’ shortcomings. In fact, given advances being made in artificial intelligence and sensor technology, we may soon be able to argue cogently for the safety of vehicles that completely drive themselves, but we would still be extremely careful about designing vehicles that *share* driving duties with the human operator.

There are already some early warning signs of shared control authority issues in the database of NHTSA’s VOQ system. In examining possible cases of UA events, the team observed a number of VOQs having to do with the misperception of UA in vehicles equipped with cruise control (a technology that could be considered “semi-smart”). Typically, these VOQs involve the engine speed increasing and the transmission downshifting, especially when the traffic flow is going uphill. In fact, the vehicle’s cruise control is functioning normally: it is maintaining speed in the presence of an increased road grade. However, because most of the manually controlled vehicles slow down on the upgrade (e.g., “dead footed” drivers), the complaining owner feels their vehicle has accelerated “of its own volition.” Put in Control Authority terms, the owner does not fully understand the authority granted to the vehicle upon engaging cruise control.

There are valuable lessons-learned regarding Shared Control Authority from other system operations domains. Automotive designers can learn from these.

While the above issues focus on vehicle design, the issue in Section 6.3.5 addresses the difficulty of gleaning reliable system performance data from either the laboratory or field reports.

6.3.5 Challenges of Studying the Human Factors Contributions to UA Events in the Lab

The first challenge in trying to study UA events in the laboratory environment is the lack of consensus as to what constitutes such an event. Some collations and analyses are limited to low-speed UA, such as those that occur in parking lots or driveways (e.g., NHTSA's Silver Book), while others include both low-speed and at-speed events. Given that different precipitating factors are more or less strongly associated with these two kinds of events, the variables studied in the laboratory will be likewise impacted by the definition of UA.

Further, laboratory studies face the challenge that UA are, in vivo, infrequent events: recreating them at their "natural" rate in the laboratory is neither time nor cost effective. Further, laboratory studies tend to focus on one class of precipitating factor: pedal misapplication. While such studies can provide an existence proof of such errors (i.e., drivers DO, in fact, step on the accelerator instead of the brake pedal) and can lend some insight into design aspects that may impact the likelihood of such errors, it is not possible to estimate the actual rate of error in the field from such studies, nor the proportion of time driver error is the primary causal factor of the UA event.

Still, empirical studies serve as a critical tool for validation of control configurations and dynamics, providing both objective performance data and subjective driver-satisfaction ratings. If, however, laboratory studies are to be employed to identify current designs that may lead to misapplications and to improve future design, certain cautions must be taken. First, investigators must be accurate in their characterizations of current designs as the manufacturing tolerances for pedal placement vary. Rather than employ a single vehicle as a representative of its class, it is incumbent upon researchers to provide a proper characterization of the parameter across the class (e.g., mean and standard deviation), and to test an appropriate sampling of that parameter's range. Additionally, manipulations that might be performed to increase the observed frequency, might compromise the ability to generalize the findings under consumers' use of the vehicle.

Second, and perhaps more critical, researchers must ensure that design modifications that address one type of driver error (e.g., brake/accelerator confusability) do not overly compromise other performance parameters. For example, given that pedal misapplication is a relatively rare error, one would not tolerate substantially longer accelerator-to-brake transition times that might accompany larger pedal separations; one must avoid having a "solution" that causes more accidents than it prevents. Once again, it is critical to examine the unintended consequences of driver interface design, as discussed in Section 6.3.3.

Ultimately, laboratory results can serve as convergent measures to validate field-test and survey data. Then, in conjunction with sound human-systems integration principles and human performance modeling, the automotive community can develop driver-vehicle interfaces that are safe and robust.

O-10. *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.*

O-11. *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.*

6.4 System Overview

The ETCS-i is responsible for controlling air flow to the engine based on driver and vehicle conditions. The ETCS-i is composed of an accelerator pedal assembly, a throttle body assembly, and an ECM. The ECM contains two CPUs, throttle motor control drive circuitry, a power supply, and inputs from other functions. In addition, the ECM electronic fuel injection and ignition functions provide fuel and spark in the correct amounts and at the correct time to keep the engine running. All three (i.e., air mass, fuel, and ignition) are needed in the correct proportion and sequence for the engine to run otherwise power output is diminished and/or the engine stalls. In addition, it takes mass air flow with the correct amount of fuel and proper ignition timing to increase the engine output power sufficiently to create UA (i.e., fuel and/or ignition spark by themselves without a commensurate amount of additional air flow cannot result in a significant power increase necessary to create UA).

The ETCS-i provides fail-safe modes serving to limit engine speed and power to a safe state in the presence of failures. Section 6.5 describes the ETCS-i defenses and responses to failures that otherwise might result in UA and/or stranding the vehicle.

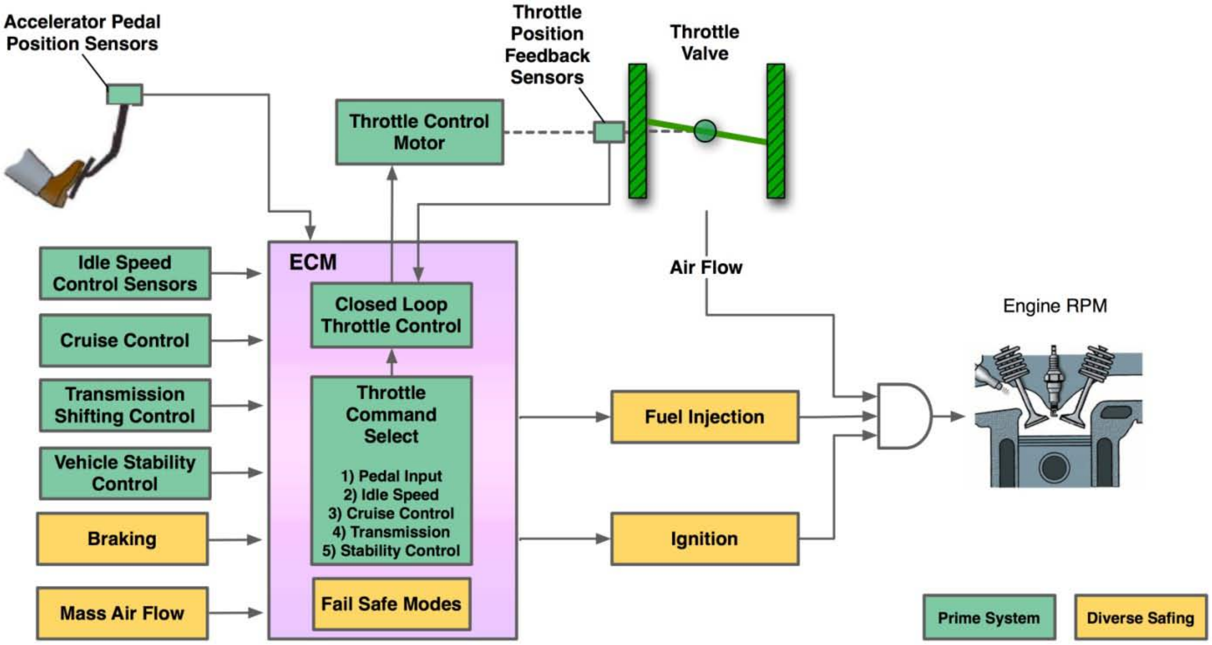


Figure 6.4-1. ETCS-i Major Functions

Figure 6.4-1 shows the major components of the ETCS-i in green and diverse safing capabilities in orange. The ETCS-i contains a closed loop throttle control function. This control loop with feedback from throttle valve position sensors adjusts the throttle valve position based on a command selected from five throttle control functions. The five major functions generating throttle commands are accelerator pedal, ISC, cruise control, transmission shifting control, and VSC.

The throttle control system utilizes sensors, electronic hardware, and software to mimic a mechanical system while providing additional features. The software contains learning algorithms to recalibrate sensor inputs as they vary over life or are influenced by environmental effects. These learning algorithms provide constant and repeatable operating characteristics for the vehicle. Learning algorithms are used in the accelerator pedal section to adjust for the equivalent of play or cable slack present in a mechanical system, ISC learns the throttle angle necessary to control engine rpm to the target idle speed considering engine environmental and load conditions, and the throttle control loop learns the sensed spring loaded detent position at engine start. Details of the learning algorithms are described in their applicable functional Section in 6.6.

The ETCS-i software also contains fault detection logic to isolate failed components and respond with an appropriate fail-safe mode that protects the vehicle from unwanted throttle opening. Multiple layers of failure detection and safe modes are employed by the software to control the engine that are not available with mechanical throttle control systems. Diverse fail-safe functions utilize fuel flow and ignition to control engine rpm and power as shown in orange in Figure 6.4-1.

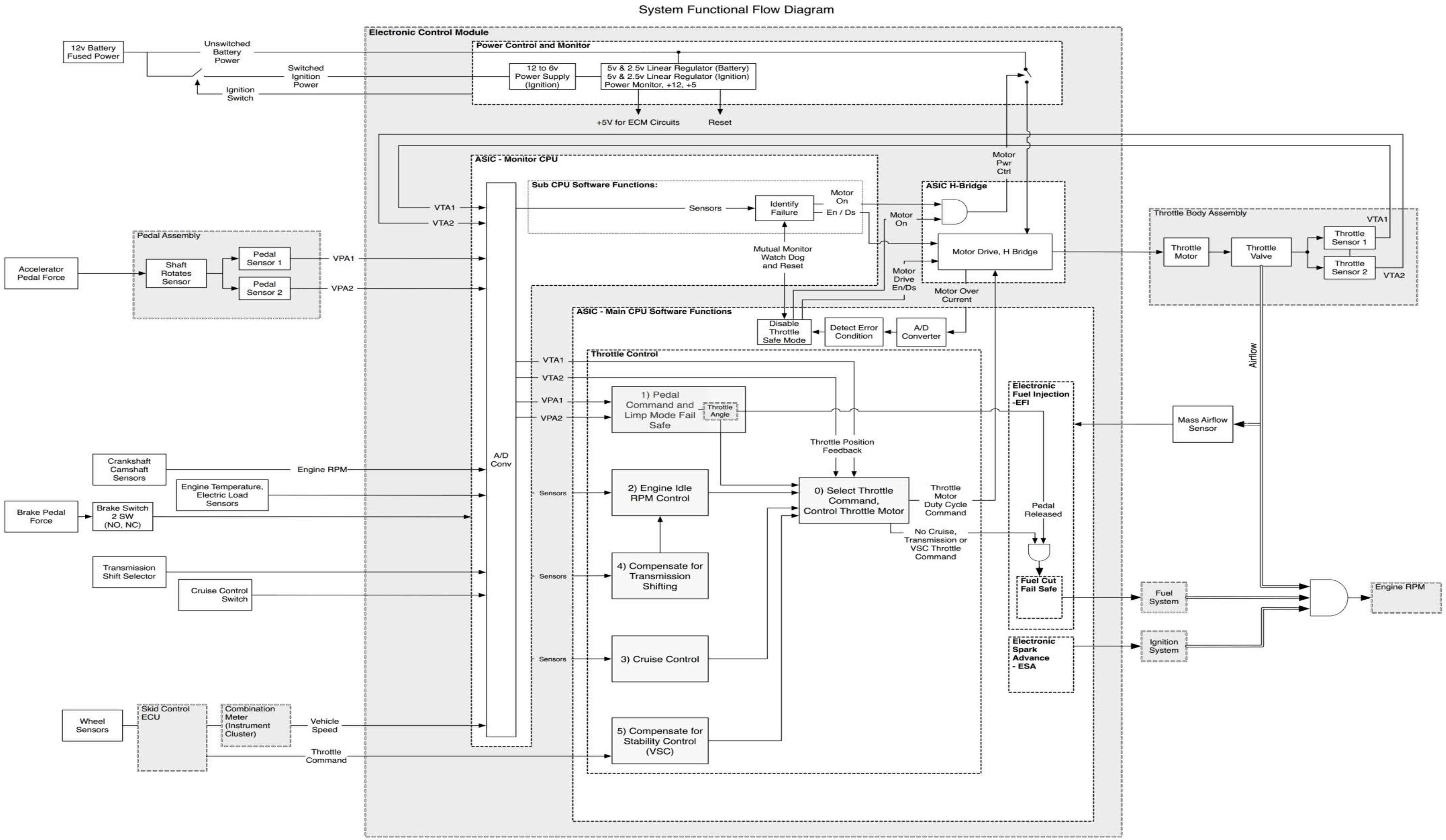
Airflow provided by the throttle is one of three critical elements enabling the engine to run as shown by the “and” gate in Figure 6.4-1. Without the proper air to fuel mixture ratio and spark to ignite the fuel the engine will not run. The ECM can utilize fuel flow and ignition as diverse ways to limit the engine speed and power independent of actual throttle valve position.

The ETCS-i provides fail-safe modes activated upon detection of failures to allow the driver to pull off to the side of the road, limp home, or safe the vehicle. A “limp home” fail-safe mode allows the vehicle to be driven at a reduced speed after some component malfunctions. If the ETCS-i components malfunction, the MIL or “check engine light” is intended to alert the driver with the malfunction stored as a DTC. If the failure is in either one of the pedal signals, the ECM will use the other pedal signal to provide limited throttle control.

The ETCS-i implements other fail-safe strategies further described in Section 6.5 when more than one signal is affected, depending on which sensor(s) fails, including operation at engine idle only, operation at a fixed throttle opening slightly more than idle with power managed through fuel flow and ignition for throttle sensor malfunctions, or engine shut down if the throttle valve is stuck or the ETCS-i determines the engine cannot be safely controlled.

6.4.1 System Design

Figure 6.4.1-1 shows an overall system functional block diagram with interfaces from sensors to actuators. The following sections describe the ETCS-i starting from the throttle body actuator towards its sensor inputs.


System Functional Flow Diagram
12v Battery Fused Power
Unswitched Battery Power
Switched Ignition Power
Ignition Switch
Electronic Control Module
Power Control and Monitor
12 to 6v Power Supply (Ignition)
5v & 2.5v Linear Regulator (Battery)
5v & 2.5v Linear Regulator (Ignition)
Power Monitor, +12, +5
+5V for ECM Circuits
Reset
ASIC - Monitor CPU
Sub CPU Software Functions:
VTA1
VTA2
Sensors
Identify Failure
Motor On
En / Ds
Mutual Monitor Watch Dog and Reset
Motor Pwr Ctrl
ASIC H-Bridge
Motor On
Motor Drive, H Bridge
Motor Drive En/Ds
Motor Over Current
Throttle Body Assembly
Throttle Motor
Throttle Valve
Throttle Sensor 1
Throttle Sensor 2
VTA1
VTA2
Pedal Assembly
Accelerator Pedal Force
Shaft Rotates Sensor
Pedal Sensor 1
Pedal Sensor 2
VPA1
VPA2
ASIC - Main CPU Software Functions
Disable Throttle Safe Mode
Detect Error Condition
A/D Converter
Throttle Control
VTA1
VTA2
VPA1
VPA2
1) Pedal Command and Limp Mode Fail Safe
Throttle Angle
Throttle Position Feedback
A/D Conv
Crankshaft Camshaft Sensors
Engine RPM
Engine Temperature, Electric Load Sensors
Brake Pedal Force
Brake Switch 2 SW (NO, NC)
Sensors
2) Engine Idle RPM Control
0) Select Throttle Command, Control Throttle Motor
Throttle Motor Duty Cycle Command
No Cruise, Transmission or VSC Throttle Command
Transmission Shift Selector
Cruise Control Switch
Sensors
4) Compensate for Transmission Shifting
Sensors
3) Cruise Control
Wheel Sensors
Skid Control ECU
Combination Meter (Instrument Cluster)
Vehicle Speed
Throttle Command
5) Compensate for Stability Control (VSC)
Airflow
Mass Airflow Sensor
Electronic Fuel Injection -EFI
Pedal Released
Fuel Cut Fail Safe
Electronic Spark Advance - ESA
Fuel System
Ignition System
Engine RPM

Not for Public Release – this document may contain sensitive and/or Toyota proprietary information
Pre Decisional: For Internal Use Only

Figure 6.4.1-1. Overall System Functional Block Diagram

6.4.1.1 Throttle Body Assembly

A throttle body diagram appears in Figure 6.4.1.1-1.The figure shows the throttle body with its valve, direct current (DC) motor, two sensors, and interfaces to the ECM.

The throttle valve regulates the volume of air entering the intake manifold. The ECM adjusts the throttle opening to a target angle based on a throttle command selected from the five major throttle control functions described below under the Main CPU software section. Two throttle position sensors mounted on the throttle body indicate the position of the throttle valve providing closed loop feedback to the throttle control loop.

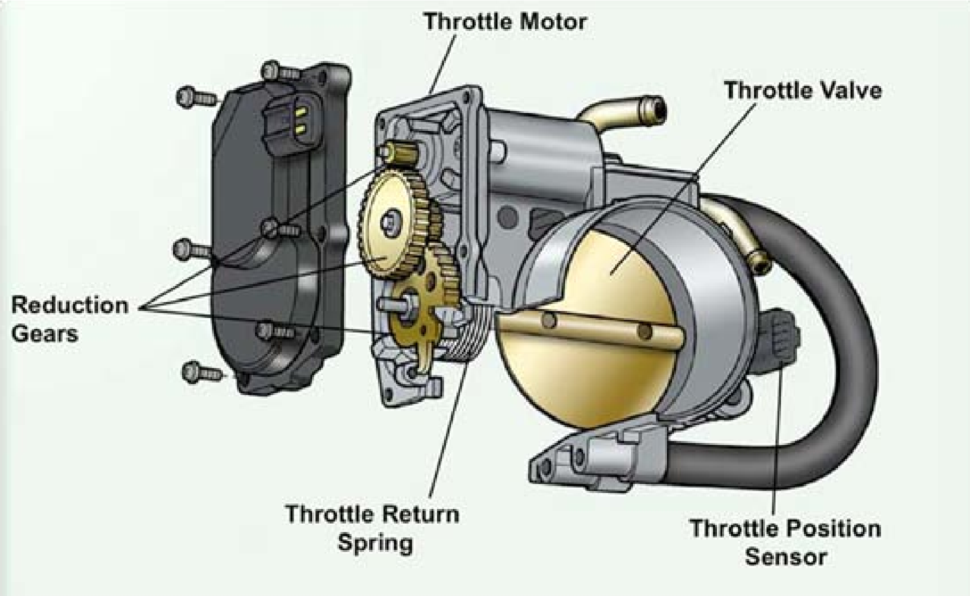


Figure 6.4.1.1-1. Typical Throttle Body Assembly (not necessarily the MY 2005 Camry)
Courtesy of TMC

The throttle control motor is a DC motor controlled by the ECM. The DC motor drives the throttle valve through a set of reduction gears. As the motor rotates the throttle valve it compresses two return springs.

Two return springs provide a detent position of 6.5 degrees from the fully closed position. Whenever the throttle motor is unpowered, the valve returns to this fixed spring detent position. This “spring detent” position provides three major functions. First, the springs keep the throttle valve from resting against the throttle body in the fully closed position. Keeping the throttle valve from contacting the throttle body throat while the vehicle is off prevents the throttle valve from becoming stuck closed[11]. Secondly, the spring detent position allows the ECM software to calibrate the throttle sensors against the mechanically known position 6.5 degrees from fully closed. Third, the spring detent position provides a fail-safe position for the throttle valve when the throttle motor is unpowered. The 6.5-degree spring detent position is about 3 to 4 degrees more open than a normal idle position. The spring detent position allows the vehicle's engine to operate slightly above idle with speed control provided by a diverse engine power management function where fuel flow and ignition timing are used to control engine power.

Current through the DC's motor's winding applies a torque against the return spring creating a near linear relationship between motor current and throttle opening. In addition, a higher current provides an even higher torque to overcome rotating friction of the throttle shaft or to overcome friction between the throttle valve and the throttle valve throat. The ECM controls the electrical current through the motor through its "H-Bridge" drive circuit. The H-Bridge circuit controls the direction of the current and the amount of current by pulse width modulating the current at 500 Hz.

Throttle Position Sensors (TPS) are mounted on the throttle and indicate the position of the throttle valve. Two types of throttle position sensors are used, depending on the vehicle MY. The TPS uses one +5V supply circuit (VC) and one ground circuit shared with the mass air flow sensor.

MYs 2002 through 2003 used Dual Output Contact Type potentiometer sensors. The TPS is built into the motor gear cover housing and mounted on the throttle body. The sensor contains two resistors and wiper arms in one housing supplied by common power and ground connections to the ECM. The TPS converts the throttle valve angle into two electrical signals (VTA1 and VTA2).

VTA1 and VTA2 increase in voltage output as the throttle shaft is rotated, but VTA2 starts at a higher voltage output and the voltage change rate is different from VTA1. Note in Figure 6.4.1.1-2 that VTA2 reaches its upper limit earlier than VTA1. The ECM uses both signals to detect the change in throttle valve position. By having two sensor signals, the ECM can compare the voltages and detect sensor problems.

[11] A common problem that occurs in mechanical throttle control systems, where the throttle plate rests against the walls of the bore when the accelerator pedal is released, is that deposits form between valve and bore, especially when the engine is turned off in a hot state. Then on a subsequent restart, when the engine has cooled, the valve is stuck in the bore. The operator has to apply high accelerator pedal pressure to free it which can cause an overshoot in intended throttle opening. If the vehicle is in gear when this happens it might lurch forward.

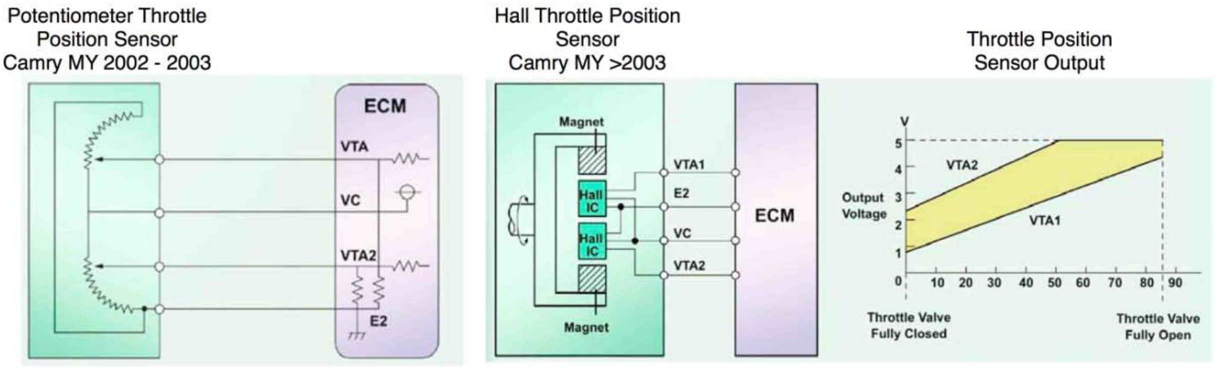

Potentiometer Throttle Position Sensor Camry MY 2002 - 2003
ECM
VTA
VC
VTA2
E2
Hall Throttle Position Sensor Camry MY >2003
Magnet
Hall IC
Hall IC
Magnet
VTA1
E2
VC
VTA2
ECM
Throttle Position Sensor Output
V
5
4
3
2
1
0
Output Voltage
VTA2
VTA1
10
20
30
40
50
60
70
80
90
Throttle Valve Fully Closed
Throttle Valve Fully Open

Figure 6.4.1.1-2. Potentiometer and Hall Effect Throttle Sensors

Courtesy of TMC

Beginning with MY 2004, the Camry used a dual output non-contact Hall Effect sensor TPS. The output voltages from the Hall Effect TPS are identical to those from the potentiometer type TPS. However, as its name implies, the non-contact type TPS does not use a wiper arm and resistor to determine the position of the throttle valve. Two Hall Effect ICs are mounted on the throttle body surrounded by a magnetic yoke. As the throttle valve moves, the yoke moves around the Hall Effect ICs, causing changes in the magnetic field. The Hall Effect ICs convert these changes into electrical signals and output them to the ECM as VTA1 and VTA2. Similar to the dual output contact type TPS, the two unique signals allow the ECM to compare outputs and detect faults. This electronic sensor is more durable than contact type sensors because it does not depend on physical contact between components and it provides a lower output impedance. The Hall Effect sensor's active analog output with a low impedance drive helps ensure the throttle signals arrive accurately at the ECM even in the presence of EMI noise and potential resistive failures.

6.4.1.2 Engine Control Module

The ECM contains two CPUs to manage the throttle, and fuel injection, ignition, emission controls, power control and monitor circuitry, and other interfacing circuitry. To operate the vehicle both CPUs must agree that the engine is operating properly. A failure in either CPU will disable the engine. As shown in the center of Figure 6.4.1-1, the ECM contains the following major sections:

a) Throttle motor control drive electronics H-Bridge

b) Main CPU ASIC and software controlling critical throttle functions

c) Sub-CPU ASIC including a common A/D converter and software functions

d) Power control and Monitor

The paragraphs below briefly describe each of the ECM sections shown in Figure 6.4.1.2-2. Additional detail is provided in Section 6.6.

a) **The throttle motor control drive electronics** ASIC and H-Bridge components interface the transistor switching pulses from the Main CPU to the throttle motor. The ASIC also contains hardware to detect high motor current and high temperature at the H-Bridge switching transistors and to automatically switch off the H-Bridge. The H-Bridge supplies an analog motor current monitor to the Main CPU for fault detection.

b) **Main CPU ASIC** and software functions are shown in the large block located in the center bottom of Figure 6.4.1.1-2. Major functions implemented in software are shown in the diagram including Throttle Control and Electronic Fuel Injection (EFI). The Main CPU also includes portions of the overall failure detection and safing modes including disabling the H-Bridge which removes power from the throttle motor returning the valve to its 6.5 degree detent position.

Analog signals that are used by the Main CPU are accessed internally by the Main CPU A/D port, or are transferred into the Main CPU via a Direct Memory Access (DMA) driven serial interface using the Sub-CPU A/D converter ports.

The Main CPU controls the operation of various electrical devices (relays, motors, solenoids, and indicator lights). In general, as actuator operation changes engine operating conditions, sensor data reflects these changes to the CPU (feedback) and the CPU continually adjusts actuator operation as required.

The Main and Sub-CPUs use two types of memory: non-volatile ROM for software code and volatile Static Ram (SRAM). The SRAM is protected by a single error detect and correct and a double error detect hardware function performed by error detection and correction (EDAC) logic.

Main CPU software functions shown in the center of Figure 6.4.1.1-2 are described below:

The *Pedal Command Function* converts two accelerator pedal position sensors inputs into a desired throttle angle command. The accelerator pedal is the only input that can command the full range of throttle motion without limit. Cruise control software limits the throttle command to achieve an acceleration limit of 0.06 g’s as sensed by changes in vehicle speed. Pedal commands are scaled from a learned null or an accelerator pedal released angle as measured by the accelerator position sensors. The pedal function also contains limp home mode logic to limit the throttle in the event of pedal sensor failures.

The *Idle Speed Control Function* is one of the more complex functions in the ETCS-i and is critical to keeping the engine running. It provides the engine enough air to start, controls engine speed during warm up, and then controls the idle speed through a learning algorithm which tracks necessary throttle angle versus speed. ISC is controlling to a mapped engine idle speed value based on conditions to maintain proper engine idle as a function of idle loads.

Idle Speed Control sets the throttle angle to achieve the desired idle speed. To maintain a target engine speed, ISC compensates and anticipates changes in engine speed by sensing coolant temperature, electric load, power steering pump load, transmission gear selection, air conditioner compressor engagement, vehicle speed, and brake switch engagement. These sensors provide information necessary to control engine speed to a constant idle speed under varying environmental conditions and engine load. Idle speed's command of the throttle is limited by a hard software limit to a maximum of 15 degree relative opening, with a maximum 11 degree relative opening based on worst case sensor inputs, and a typical ISC of 3 degrees. ISC also accepts a maximum of a 5 degree desired throttle command from the transmission shifting function.

Cruise Control receives inputs from the cruise control switch located on the steering column along with transmission gear selection, brake engagement, and vehicle speed sensors to maintain and modulate vehicle speed without accelerator pedal inputs. Cruise control disengages when commanded, or by activating the brake switch, shifting to neutral, vehicle speeds below 25 mph, or slowing more than 9 mph below the set speed. Cruise control commands the throttle to the degree necessary to maintain the set speed; however, it is limited in software to a maximum 0.06 g's acceleration.

Transmission Shifting utilizes engine speed and transmission gear selection to modulate the throttle to smoothly shift from one gear to another. This function also applies some throttle during torque convertor lock up to limit shuddering. Transmission shifting throttle control is limited by software to a 5 degrees relative opening and added in as part of ISC.

VSC receives vehicle speed input from each wheel and adjusts throttle valve angle to help maintain traction. Prior to MY 2007, the VSC could only reduce the throttle command and therefore cannot command any opening of the throttle. Traction control is a sub component of VSC.

Throttle Control authority for each of the five throttle control functions varies according to Table 6.4.1.2-1. Only the pedal control function has sufficient control authority to fully open and maintain the throttle in this position.

Table 6.4.1.2-1. MY 2005 Throttle Control Limits

Throttle Control Function	Throttle Control
1) Accelerator Pedal	Full Control. 0 to 84 degrees
2) Idle Speed Control	15 degrees relative maximum limited by software, typical values 3 degrees – 5 degrees maximum from idle speed sensors is 11 degrees. Idle speed accepts a maximum 5 degree transmission shifting input before applying the 15 degree maximum.
3) Cruise Control	Full Control to achieve 0.06 g acceleration. Typical 10 degrees change, but depends on incline and transmission gear.
4) Transmission Shifting Control	Limited by software to 5 degrees and added as part of idle speed
5) VSC	Limited to closing throttle

c) **The Sub-CPU ASIC** shown in the center and left of Figure 6.4.1.1-2 includes two A/D converters, microcontroller, interfaces, and software functions.

For ETCS-i, the Sub-CPU only detects and issues diagnostic codes related to Main CPU performance and Throttle Motor Performance. The Sub-CPU does not run duplicate logic and compare with the Main CPU or run diagnostics on the raw sensor values it receives. The Main CPU and the Sub-CPU share data across the serial interface and these diagnostic comparisons verify proper CPU software operation.

The Sub-CPU software performs system level self-diagnostic checks and stores Diagnostic DTCs if problems are found. System level checks are performed on input data to the Main and Sub-CPUs and set fault codes that can disable the throttle motor power feed through an interface to the ECM Power Control and Monitor Circuitry.

A heartbeat/watchdog exchange between the Main-CPU and Sub-CPU detects major CPU failures and can reset the CPUs. If the Sub-CPU flags a critical fault code it can disable the throttle motor power feed through an interface to the ECM power control and monitor circuitry which activates a limp home mode.

The Sub-CPU must be functional to provide power to the throttle motor. The Main CPU must be functional to generate the Pulse Width Modulator (PWM) waveform to drive the throttle motor. Any reset to either CPU disables the throttle motor in hardware.

Three A/D converters are used to convert engine-operating conditions sensors (such as temperature, engine speed, throttle position, and other factors) into digital words for use by both Sub and Main CPUs.

The Sub-CPU has memory mapped I/O access to two A/D converter ports, one 10 bit and one 12 bit. The Main CPU has memory mapped I/O access to a third A/D converter. Analog signals that are used by the Main CPU are accessed internally by the Main CPU A/D port, or are transferred into the Main CPU via a DMA driven serial interface using the Sub-CPU A/D converter ports.

The Sub-CPU does not perform the functional processing, but performs hardware sensor input functions and limit checks. The Sub-CPU produces fault codes based on these limit checks.

For the MY 2005 Camry ETCS-i DTCs, the Main CPU diagnostics are responsible for issuing 24 codes, and the Sub-CPU diagnostics are responsible for issuing 5 codes.

d) **Power Control and Monitor** The top portion of the ECM block shown in Figure 6.4.1-1 shows the major power distribution functions. Two types of power are supplied to the ECM: unswitched battery power (+B) and switched power (IG) controlled by the ignition switch.

The ECM provides multiple regulated 5V supplies referred to as “Vc”. [redacted]

The VC (+5 supply) has foldback current limiting. One unswitched +5V from the unswitched +12V, and +5V and [redacted] switched from the +12 ignition switch is used by the ECM processors. The VC +5V feeds are used by many engine sensors including mass air flow and the throttle and accelerator position sensors.

Power control also detects low voltage of the +12V at 8V and resets the CPUs when the +5V drops to a low values of 4.5V a low voltage signal watchdog interrupt (WI) activates and power control performs a reset at 3.7V.

6.4.1.3 Accelerator Pedal

The left side of Figure 6.4.1.3-1 shows the Accelerator Pedal Positioning Sensor (APPS) mounted to the accelerator pedal. As the driver moves the accelerator pedal, the APPS signal voltage changes to indicate pedal position. There are two voltage output signals from the APPS, VPA1 and VPA2. The ECM uses the two pedal sensors to interpret the driver’s command and then calculates the desired throttle valve angle. Also, by using two signals, the ECM is able to compare and detect if there is anything wrong with APPS performance. The two pedal sensors are supplied by individual power and ground interfaces to the ECM to maintain their independence and functional redundancy.

MYs 2002 through 2006 used a dual output contact potentiometer type APPS, shown in Figure 6.4.1.3-1. The potentiometer is mounted on the accelerator pedal bracket and contains two resistors and wiper arms in one housing. The APPS converts the accelerator pedal movement and position into two electrical signals (the APPS produces dual outputs).

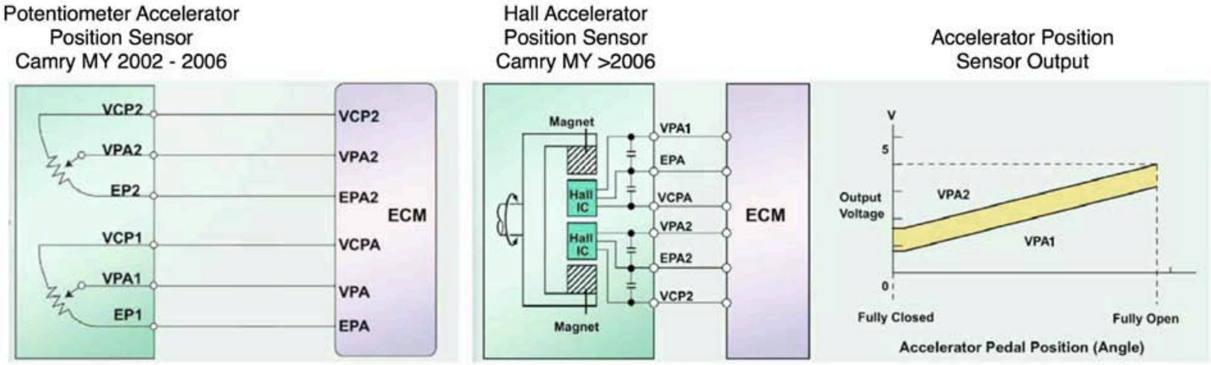

Potentiometer Accelerator Position Sensor Camry MY 2002 - 2006
VCP2
VPA2
EP2
VCP1
VPA1
EP1
VCP2
VPA2
EPA2
VCPA
VPA
EPA
ECM
Hall Accelerator Position Sensor Camry MY >2006
Magnet
Hall IC
Hall IC
Magnet
VPA1
EPA
VCPA
VPA2
EPA2
VCP2
ECM
Accelerator Position Sensor Output
V
5
Output Voltage
VPA2
VPA1
0
Fully Closed
Fully Open
Accelerator Pedal Position (Angle)

Figure 6.4.1.3-1. Accelerator Pedal Positioning Sensor

Courtesy of TMC

The wiper arm is always in contact with the resistor and moves with the accelerator pedal. The available voltage at the point of contact between the arm and resistor is sent through the VPA1 and VPA2 wires to the ECM and interpreted as accelerator pedal position.

VPA1 and VPA2 increase in voltage output as the accelerator pedal is depressed, but VPA2 starts at a 0.8V higher output voltage. The voltage slope with pedal angle is the same as VPA1. Note in the graph that VPA2 reaches its upper limit earlier than VPA1. The ECM uses both signals to detect the change in accelerator pedal position. By having two signals in one sensor, the ECM can compare the voltages and detect sensor problems.

TMC uses dual output non-contact Hall Effect sensors in MY 2007 Camry and beyond**.** The output signals voltages from a non-contact Hall Effect sensor APPS are identical to those from a contact type potentiometer APPS. The non-contact APPS does not use a wiper arm and resistor to determine the position of the throttle valve. As the accelerator pedal moves, a magnetic yoke moves causing changes in a magnetic field around the Hall ICs. The Hall ICs convert these changes into electrical signals and output them to the ECM as VPA1 and VPA2. Like the dual output contact type APPS, the two unique signals allow the ECM to compare output and detect faults. The Hall Effect sensor does not depend on physical contact between a wiper and a resistive element and also provides a lower output impedance. The Hall Effect sensor's active analog output with a low impedance drive helps ensure the throttle signals arrive accurately at the ECM even in the presence of EMI noise and potential resistive failures.

6.4.2 Throttle Control and Effects on Acceleration and Braking

Key question number 5 from NHTSA asked, "Could the *(electronics)* failure have any effect on other interfaces, such as braking system?" With the help of NHTSA expertise, the NESC assessment explored electrical and functional interfaces between ETCS-i and braking.

A large fraction of the VOQs indicate that the vehicle accelerated and brakes reportedly were unable to bring the vehicle to a stop, see Section 6.2.4. Fundamentally the braking system is a hydraulically actuated system which is separate from the ETCS-i. The NESC team did not find an electrical path from the ETCS-i that could disable or affect the brake system.

For most vehicles equipped with vacuum power brake assist since the 1970’s there is a functional linkage between throttle position and braking via the vacuum based power brake assist function. Engine vacuum from the intake manifold is stored in a reservoir, and is used by the power brake booster to amplify the driver’s force (approximately a factor of 5) on the brake pedal thus increasing the net braking force.

With a depleted vacuum reservoir, the power brake assist is lost resulting in increased stopping distance or the necessary application of additional brake pedal force to achieve a similar stopping ability. Power brake assist vacuum gets depleted when the driver releases the brake pedal after an application. The vacuum replenishes itself from the intake manifold vacuum when the brake is fully released. If the throttle is wide open the intake manifold supplying vacuum decreases. If the brake is repeatedly pressed or pumped while the throttle valve is open, then the vacuum may not replenish itself, depending on how hard the pedal is displaced. After the second or third application of the brake, the vacuum reservoir will typically be depleted if the throttle valve is wide open.

***F-3**. The NESC study and testing did not identify any electrical failures in the ETCS-i that impacted the braking system as designed.*

a. At large throttle openings (35 degrees 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.

At the request of the NESC team, NHTSA evaluated a MY 2005 Camry V6 to characterize vehicle deceleration as a function of throttle opening with a depleted vacuum system. NHTSA’s testing indicates that the MY 2005 Camry vehicle with depleted vacuum could be decelerated at 0.25 g with 112 lb_f [12]on the brake pedal, with a throttle opening of less than 30 degrees above idle, or less than 24 degrees above idle while at worst case gross vehicle weight rating. Therefore, a relative throttle opening of 25 degrees above idle or 35 degrees absolute is used for characterizing the amount of throttle opening necessary to match the reported symptoms of large acceleration with impaired braking ability.

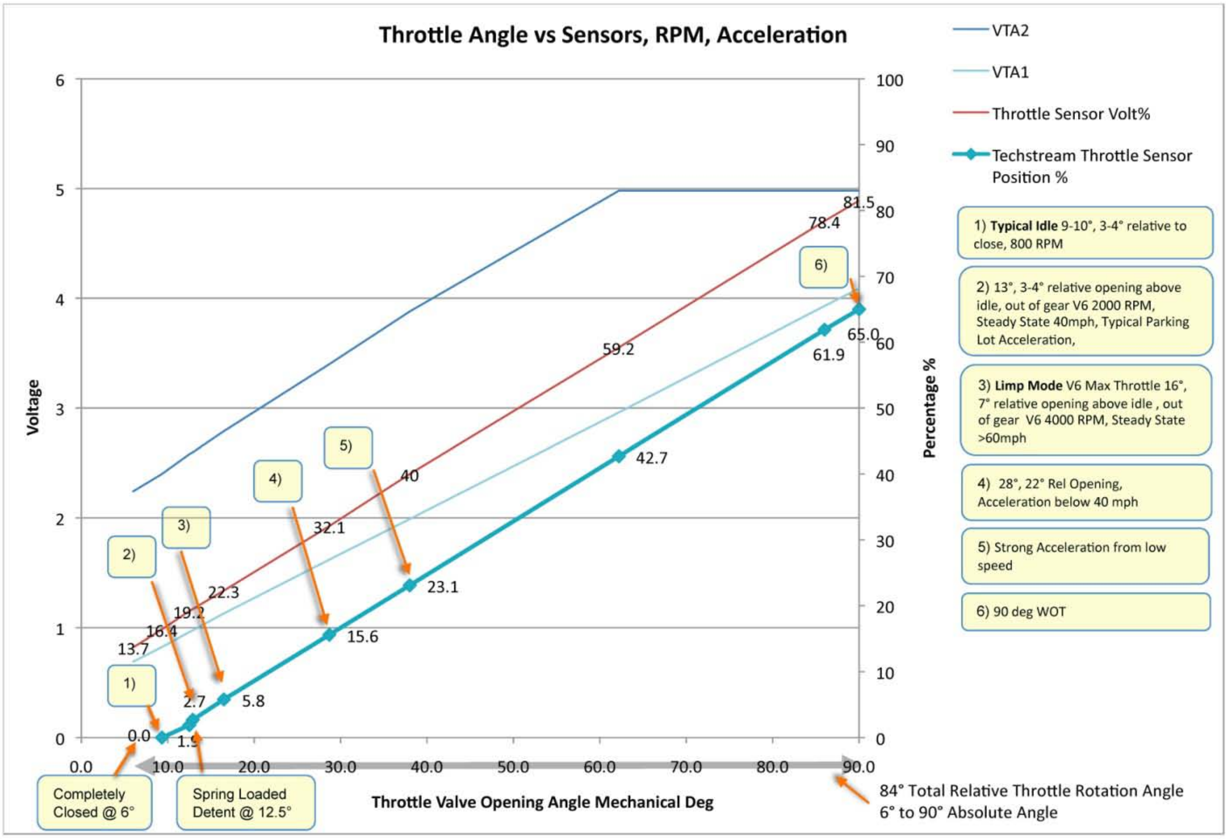
***F-8.a.** NHTSA demonstrated that a MY 2005 Camry with a 6 cylinder engine can be held in a stopped condition with a brake pedal force of approximately 10 lb_f with throttle openings up to 5 degrees.*

6.4.2.1 Throttle Opening Effects

The throttle valve operates over an 84 degree range of motion from the fully closed position to

[12] Referenced in the FMVSS135 Standard

wide open when the butterfly valve is oriented parallel to the air flow. The fully closed position is 6 degrees from perpendicular to the nominal wide open airflow. Figure 6.4.2.3-2 plots the throttle valve angle against the VTA1 and VTA2 voltages as well as a percentage of VTA1 with 5V representing 100 percent.



1) **Typical Idle** 9-10°, 3-4° relative to close, 800 RPM

2) 13°, 3-4° relative opening above idle, out of gear V6 2000 RPM, Steady State 40mph, Typical Parking Lot Acceleration,

3) **Limp Mode** V6 Max Throttle 16°, 7° relative opening above idle , out of gear V6 4000 RPM, Steady State >60mph

4) 28°, 22° Rel Opening, Acceleration below 40 mph

5) Strong Acceleration from low speed

6) 90 deg WOT

Completely Closed @ 6°

Spring Loaded Detent @ 12.5°

84° Total Relative Throttle Rotation Angle
6° to 90° Absolute Angle

Figure 6.4.2.3-2. Plots throttle valve angle against the VTA1 and VTA2 voltages and percentage of VTA1

6.4.3 Summary of Hardware Evolution

Electronics components associated with engine control were present before the introduction of the ETCS-i. These included items such as throttle position sensors, cruise control systems, and voltage regulators for sensors. At the inception of the ETCS-i for the MY 2002 Camry, some of these components naturally migrated into the new system along with new components such as accelerator pedal position sensors and the throttle valve motor driver. Since the ETCS-i introduction in 2002, the hardware, software and overall design have continued to evolve. Table 6.4.3-1 describes the Hardware Configuration Evolution for the Camrys L4 and V6 from MY 2002 through 2007.

Table 6.4.3-1. Hardware Configuration Evolution

Camry's Electronics Throttle Control (ETC) Hardware Evolution summary

Component	Model	Model Year					
		2002	2003	2004	**2005**	2006	**2007**
Accelerator Pedal Position Sensors	L4	2 potentiometers, parallel configuration					2 Hall Effect sensor, parallel configuration
	V6						
Throttle Position Sensors	L4	2 potentiometers, series configuration		2 Hall Effect sensor, parallel configuration			
	V6	2 potentiometers, parallel configuration					
Motor Drive Ckt	L4	H Bridge with two internal FETs with current sense and 3 FET Switches.					
	V6	H Bridge with only internal FETs	H Bridge with two internal FETs with current sense and 3 FET Switches.				
Voltage Regulators	L4	One voltage regulator IC, with common 5 v supply (VC)					
	V6						
Cruise Control I/F	L4	Resistive ladder network, with4 contacts to gnd					
	V6						
Main ASICs	L4	3 Main Application Specific Integrated Circuits (ASICs)		2 Main ASICs			
	V6	3 Main ASICs					2 Main ASICs

1) Accelerator Pedal Position Sensor: From MY 2002 through 2006, the system relied on two independent, but mechanically coupled, potentiometers for sensing the accelerator pedal position. This was changed in 2007 and thereafter to two electrically-independent non-contact Hall Effect sensors. This is true for the L4 and V6 models.

2) Throttle Position Sensor: From MY 2002 through 2003 the system relied on two independent, but mechanically coupled potentiometers for sensing the throttle position. This concept migrated from previous mechanical throttle system where the position was sensed by a single potentiometer. This was changed in 2004 and thereafter to two electrically-independent non-contact Hall Effect sensors. This is true for the L4 and V6 models.

3) Motor Drive Circuit: Although there have been changes in the electrical components used for this circuit, the basic Motor Drive Circuit architecture has remained unchanged since its inception. Prior to MY 2003, the H-Bridge transistors that switched to ground were located inside the ASIC. The motor drive ASIC is based on Silicon on Insulator (SOI) substrate. SOI substrates can allow higher switching speed (or lower power switching at original speed), improved reliability through suppression of latch-up, a higher tolerance to radiation, a higher breakdown voltage, and operation at higher temperature.

4) Voltage Regulators: Although there have been changes in the electrical components used for this circuit and different voltage levels for some CPUs, the basic voltage regulator architecture has remained unchanged since its inception. This is true for the L4 and V6 models.

5) Cruise Control Interface (I/F): The Cruise Control I/F architecture has remained unchanged since its inception prior to ETCS-i. This is true for the L4 and V6 models.

6) Main ASICs: The ECM functionality resides within the ASICs, which contain analog-to-digital converters, serial communication interfaces, memory, and CPU. The MY 2005 Main CPU uses 2.5V and the MY 2007 and later uses 1.2V. The combination of these ASICs, the associated software and the external peripherals enables the full operation of the ETCS-i. Although there have been changes in the ASIC design and quantities per ECM, the main functionality has remained unchanged. In 2004, advances in the electronics industry enabled larger integration of electrical components within smaller physical area, thus allowing the physical reduction of ASICs within the ECM while keeping the same functionality. This triggered changes in the number of ASICs used in the L4, and later in MY 2007 on the V6 models.

6.4.4 The Role of Diagnostic Trouble Codes

“Computers in automobiles” dated back to 1969 when Volkswagen introduced the first on board CPU with scanning capability. In 1975 a simple On-board Diagnostic (OBD) was implemented on the Datsun 280Z, followed later by other manufacturers such as General Motors, when they implemented, in 1980, a proprietary interface and protocol for testing the ECM. This interface and protocol was implemented on California vehicles in the 1980 MY, and the rest of the United States in 1981, but was not intended for use outside the factory. In 1987, the California Air Resources Board required that all new vehicles sold in California from 1988 (MY1988) have some basic OBD capability (OBD-I). In 1988, the Society of Automotive Engineers recommended a standardized diagnostic connector and a set of diagnostic test signals. In 1994 the Clean Air Act asked that 1994 and later model vehicles be equipped with “onboard diagnostic systems”, featuring dashboard warning lights that alert drivers to malfunctioning emission control equipment and be capable of storing trouble codes that help automotive technicians pinpoint the malfunction. It was not until 1996 that the government mandated for all vehicles sold in the United States the OBD-II specifications[13]. This mandate included specific DTCs (targeted to help troubleshoot the emission control system) and allowed room for vendor-specific codes.

Table 6.4.4-1 illustrates the Camry’s DTCs evolution since the introduction of the ETCS-i up to MY 2007. For the MY 2002 Camry there were only a few DTCs, but these codes were changed/expanded from MY 2003 and thereafter. In 2008 (not shown), the DTCs for the V6 model ECM (P0606 and P0607) were further expanded. That is, in MY 2003, a single code covered multiple fault conditions which were in later MYs separated into individual codes.

[13] SAE J 2012 and Toyota's 874_EngCtrlSys-II_TechHdbk_04-16-08

Table 6.4.4-1. Diagnostic Trouble Codes

Component	Description	MY						CPU	
		2002	2003	2004	2005	2006	2007	Main	Sub
Accelerator Pedal Position Sensor	VPA1 Chattering, Intermittent Open / Short	P1120	P2120					X	
	VPA1 Low Voltage, open, ground short		P2122					X	
	VPA1 High Voltage, short to +V		P2123					X	
	VPA2 Chattering, Intermittent Open / Short		P2125					X	
	VPA2 Low Voltage, open, ground short		P2127					X	
	VPA2 High Voltage, short to +V		P2128					X	
	VPA1-VPA2 Correlation, VPA1 to VPA2 short, Both VPA1 and VPA2 open		P2138					X	
	VPA1-VPA2 Rationality Approx 1.2<VPA2-VPA1<.4	P1121	P2121					X	
Throttle Position Sensors	VTA1 Chattering	P0120	P0120					X	
	VTA1 Low Voltage		P0122					X	
	VTA1 High Voltage		P0123					X	
	VTA2 Chattering		P0220					X	
	VTA2 Low Voltage		P0222					X	
	VTA2 High Voltage		P0223					X	
	VTA1-VTA2 Correlation		P2135					X	
	VTA1-VTA2 Rationality	P0121						X	
Throttle Motor Drive Circuit	Throttle Actuator Stuck Open	P1128	P2111					X	
	Throttle Actuator Stuck Closed		P2112					X	
	System Guard No. 1	P1129	P2119					X	X
	System Guard No. 2							X	X
	System Guard No. 3							X	X
	Throttle Actuator Control Motor Circuit Low	P1125	P2102					X	
	Throttle Actuator Control Motor Circuit High		P2103					X	
	Throttle Actuator Supply Voltage Circuit Low	P1127	P2118						X
Electronics Control Module	Throttle Actuator Supply Voltage Circuit Open (PMOS abnormality)	P1633	P0657					X	
	Control CPU error		P0607						X
	Monitor CPU error								X
	TP sensor input circuit error		P0606						X
	APP sensor input circuit error								X
	Cruise CPU error								X
	Peripheral circuit (ESP, AD) error								X
	RAM error		P0604					X	

6.5 System Fail-Safe Architecture

The ETCS-i provides multi-layered design features against failures and responds with fail-safe modes to reduce the likelihood of UA and/or stranding the vehicle. Both UA and stranding have safety implications. Shutting the vehicle off might be one response to a failure threatening UA; however, stranding the vehicle might introduce a new hazard. Therefore, responses balance the ability for the vehicle to safely remain mobile versus immobilizing and stranding the vehicle.

Basic failure detection starts with a layer of sensor and throttle actuator checks that generate a DTC. These DTCs initiate limp home modes, which keep the vehicle mobile under reduced engine power and limit engine speed. These limp home modes at reduced engine power protect the vehicle from stranding under certain failure conditions.

To protect the vehicle from UA under normal operating conditions or while limp home modes are in effect, the TMC ETCS-i includes a fuel cut feature that limits engine speed to under 2500 rpm when the pedal position sensors indicate that the accelerator is not pressed. The fuel cut safety feature provides an umbrella to defend against failures that may escape detection by the lower level DTCs that monitor individual sensors, the throttle actuator, and CPU monitors for cases where the ECM senses the accelerator is not pressed.

> ***F-2.*** *Safety features are designed into the TMC ETCS-i to guard against large throttle opening UA from single and some double ETCS-i failures. Multiple independent safety features include detecting failures and initiating safe modes, such as limp home modes and fuel cut strategies.*

The NESC team examined the architecture of the TMC ETCS-i to identify built in fail-safe features and how multiple sensors and CPUs are utilized to guard against the vehicle from UA and/or stranding.

The ETCS-i utilizes sensors, electronic hardware, and software to mimic a mechanical system where a cable from the accelerator connects to the throttle. A benefit of an electronic throttle control system is that it does not suffer from the wear out failures present in a mechanical system. However, electronic control can introduce different types of risks. Therefore, the ETCS-i provides fail-safe modes to limit engine speed and engine power to a safe state to manage the risks.

Both internal environments (such as vibration and temperature) and external environments (such as EMI and moisture) conceptually have the potential to induce vehicle failures. Additionally, some failures might propagate from one system into the ETCS-i, such as fluid leaks from the cooling, lubrication, or hydraulic systems possibly affecting electrical connections.

To respond to such failures, the ETCS-i employs three fail-safe strategies, a set of limp home modes, engine power limiters, and a complete vehicle shut off. These are summarized below and described in detail in Section 6.5.2.

The system employs some over arching design features against stranding and unintended throttle opening. These envelope and mitigate the consequences of many lower level mechanical and electrical failure modes. Fail-safe features employ 1) returning the throttle valve to or near the idle position, where the braking system can overcome the resulting engine power, 2) cutting the fuel supply and modulating ignition to limit engine power, or 3) shutting off the engine.

The system detects failures such as a mechanically stuck throttle valve that the ETCS-i cannot overcome. Methods used to detect a stuck throttle valve include high motor duty-cycle, and high current or with high temperature at the motor drive transistors. Upon detecting a stuck throttle valve that is in the wrong position and cannot be moved, the electronics limits engine speed to idle by withholding fuel and ignition through a fuel cut function. If the throttle valve subsequently moves resulting in too high of a mass air flow, then the engine is shut off.

Fail-safe fuel cut employs a method of engine control diverse from throttle valve rotation. The diverse fuel cut provides a defense against a large number of mechanical throttle and electrical faults that might otherwise result in high engine speed and unwanted power levels. The ETCS-i employs a fuel cut feature to limit engine speed under 2500 rpm when the accelerator pedal is sensed as released. This fail-safe strategy provides an overarching mechanism that protects the vehicle from failures in the throttle body itself and the electronics that drives the throttle. Idle speed fuel cut can respond to failures escaping throttle motor position, duty cycle, and high current detection features mentioned above.

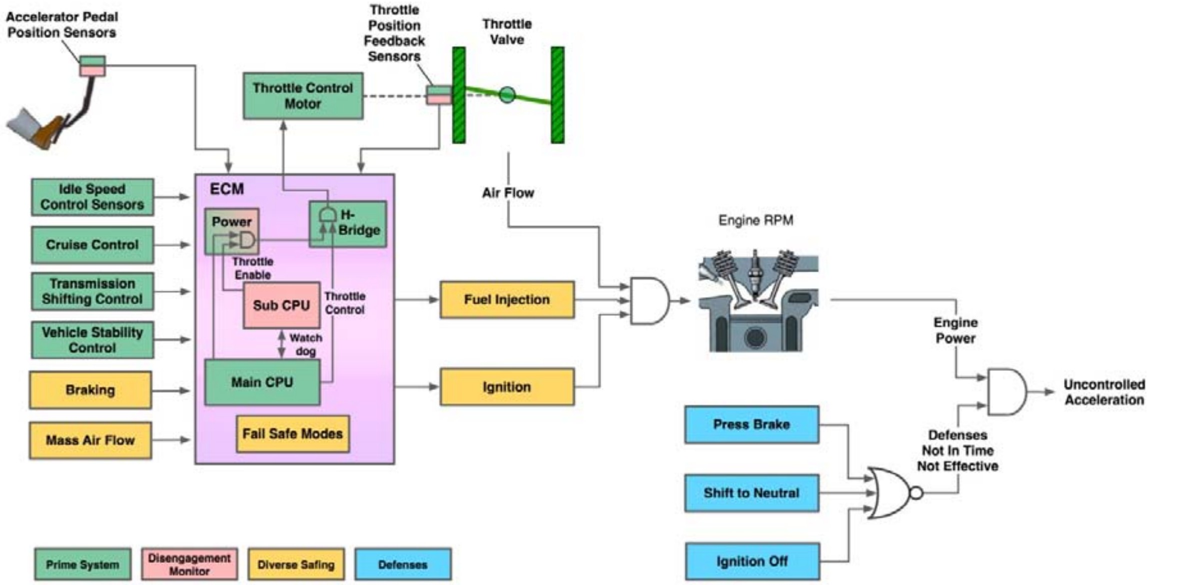


Figure 6.5-1. Overall Architecture – Prime System with Disengagement Monitor and Diverse Safing Control

As noted in Figure 6.5-1, there are four main control elements of the integrated system. The green blocks show the prime system elements controling the throttle. The prime system is a simplex system including prime sensor functions, Main CPU and the H-Bridge that drives the throttle motor controlling throttle valve position. The pink blocks show the disengagement monitor function consisting of a second set of sensors, the Sub-CPU, and its path to disengage power to the H-Bridge controlling the throttle motor should a fault occur. Architecturally, the system appears as a simplex system with disengagement monitor[14] and diverse safing. Without power the throttle cannot be driven and dual springs return the valve to a near idle position as required by Federal Motor Vehicle Safety Standards (FMVSS) 124, 6.5 degrees from fully closed. The orange blocks show the diverse fuel cut method of engine speed control through fuel and ignition modulation or total fuel cut off should the throttle become inoperable. The fourth element shown in blue, captures the primary defenses against UA available to the driver beyond the system fail-safe design features. These defenses are outside the ETCS-i and are possible operator overrides that include applying the brakes, shifting to neutral, and/or turning the ignition off.

O-1. 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 drivers may not know or understand the vehicle response for the hazard controls at their disposal and how to use them. For example:

a. Shifting to neutral with the resulting high engine speed will not harm the vehicle.

b. Pumping the brakes can decrease their effectiveness.

c. Turning the vehicle off while driving may require a different sequence than when the vehicle is stopped and will not lock the steering wheel.

d. 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.

6.5.1 System Redundancy

For the purposes of this report, redundancy is defined as “the use of more than the required minimum number of components, in order to increase the system reliability.”[15] Understanding how reliability (or failure) is defined in the context of the functions necessary to operate the ETCS-i is critical for determining whether and how the system provides redundancy. How sensors are logically combined and used to perform the functions will determine if it can operate at a higher reliability than a single string or single item system.

Figure 6.5.1-1 shows sensor and actuator interfaces to the ECM and their critical functions implemented in hardware and software. The prime system’s actuation path starts at the accelerator pedal, proceeds through the Sub-CPU A/D converter section, through the Main CPU

[14] Hammett, Robert, Design by Extrapolation an Evaluation of Fault-Tolerant Avionics, The Charles Stark Draper Laboratory, Inc., Cambridge, A44, p1.C.5-4

[15] C. (Raj) Sundararajan, Guide to Reliability Engineering, Van Nostrand Reinhold, New York, © 1991. p. 90

to the throttle motor and valve controlling airflow to the engine. The main throttle valve position feedback control path starts at the throttle position sensors, passes through the A/D converters, and ends at the throttle control function.

Fundamentally, the ETCS-i uses two sets of sensors and CPUs to control the throttle and disengage the throttle control function when the sensors or CPUs do not agree. The prime sensors (VPA1 and VTA1) and the Main CPU control the intended throttle opening. The second sensors, VPA2, VTA2, and the Sub-CPU are used to validate consistent sensor data and a properly operating Main CPU. Both CPUs must agree that the throttle motor should be engaged in order for the throttle motor to drive the throttle valve open.

While the second sensors and CPU do not directly provide a means for driving the throttle, both pedal sensors are needed to indicate off idle in order to open the throttle. Either pedal sensor, throttle sensor, or CPU can declare a fault and disable and/or disengage the throttle. These sensors and CPUs are in "series" to open the throttle.

The two sensors and two CPUs are functionally arranged in a series manner, as described above, providing for two methods for closing the throttle. This prevents the failure in a single circuit or CPU from opening the throttle unexpectedly.

If a failure is declared in either VPA1 or VPA2, the limp home mode is entered and the other sensor is used to control the throttle valve albeit at a limited relative opening of 10 to 15 degrees, depending on engine type, maximum that provides limited engine power.

The two pedal sensors must agree and both are necessary to open the throttle. Since both sensors are necessary to open the throttle the system is redundant to closing the throttle, but not opening the throttle. However, if one sensor is declared failed, then a limp home mode is entered, and the other working sensor is used to control the throttle over a limited 10 to 15 degrees range. In the event the system detects and isolates the failure of one pedal sensor, the system is considered redundant to continuing to operate the vehicle albeit with reduced power.

The Main CPU and Sub-CPU must be functioning and must agree that the throttle motor can be driven. Each CPU has its own oscillator, memory error detect and correct along with a watchdog that can reset the processor. The CPUs also communicate with each other to assure that both receive consistent sensor data and are functioning properly. If either CPU fails, throttle motor drive is disabled. The system is redundant to preventing a failed Main CPU from controlling the throttle.

Two throttle sensors need to agree that the throttle valve is positioned properly. If the throttle valve does not achieve its intended position, power to the throttle motor is shut off. When the throttle position sensors disagree, throttle control is disabled and the throttle valve is returned to a spring loaded detent position of 6.5 degrees opening which is about 3 degrees more open than typical warm idle. At this point the diverse fuel cut function controls engine speed. Multiple sensors and signal sources are used to identify if the throttle motor is having trouble driving the throttle to its intended position. The motor current is measured with automatic hardware trip thresholds switching the H-Bridge off and software monitoring of the current to disable the motor power. In addition to hardware over current trip, a hardware over temperature trip can also disable the H-Bridge. CPU controlled pulse width modulator duty cycle is monitored and the H-Bridge is turned off if the duty cycle is too high.

Diverse backup controls utilizing the Electronic Fuel Injection (EFI) module limit engine speed and power through a power management function employing fuel cut and ignition timing to protect the system against the consequences of unintended throttle opening due to the failure of sensors, CPU, or a mechanically stuck open throttle valve or otherwise mechanically failed throttle valve. The diverse backup is the fuel cut function that will stop fuel flow to the engine if either VPA1 or VPA2 indicate idle and the engine speed is above 2500 rpms.

6.5.2 System Failures

System failures resulting in high engine speed or power are captured in the High Level Functional Fault Tree shown in Figure 6.5.2.1-2. Many electronic throttle system failures are detected and mitigated by lower level sensor or actuator fail-safe detection mechanisms that generate DTCs. Lower level fail-safe detection mechanisms are identified with blue boxes in the more detailed Functional System Level Fault Tree shown in Figure 6.5.2.2-1.

System level fail-safe strategies serve to control failures escaping detection at a lower level that potentially can result in high or uncontrolled engine speed or power. Idle Speed Fuel Cut is one such strategy limiting the engine speed to 2500 rpm when at least one of the two accelerator position sensors indicates idle or foot-off pedal. This strategy is shown in yellow in the middle of Figure 6.5.2.2-1.

The left side of Figure 6.5.2.2-1 shows failure modes resulting in high engine speed/power when the system senses an accelerator pedal command or accelerator pedal pressed conditions. Failures on the left branch appear as valid pedal signals, therefore they are difficult to identify and mitigate at either lower levels or at the system level.

Two paths with postulated failure causes were found that could open the throttle more than 25 degrees above idle. One path requires a specific set of resistances in order to recreate the postulated accelerator pedal pressed condition. This engineered failure mode typically requires two good connections to fail in a precise manner. Physical evidence of these engineered failure modes were not found in the examination of VOQ vehicles. The second path requires an undetected software malfunction.

1) The first path involves creating two failures in the VPA1 and VPA2 signal paths. Fundamentally both signals must fail in the operational lane appearing as valid accelerator pedal positions. See Section 6.6.2 for a detailed description of this failure mode and definition of “operation lane” in Section 6.6.1.1.
2) The second path involves a malfunction of the Main CPU that unilaterally opens the throttle when the accelerator pedal is not pressed while performing the following functions correctly:

a) fuel injection and ignition timing operating properly

b) proper servicing of the watchdog timer so it does not detect a failure

c) proper communication with the Sub-CPU so it does not detect the failure

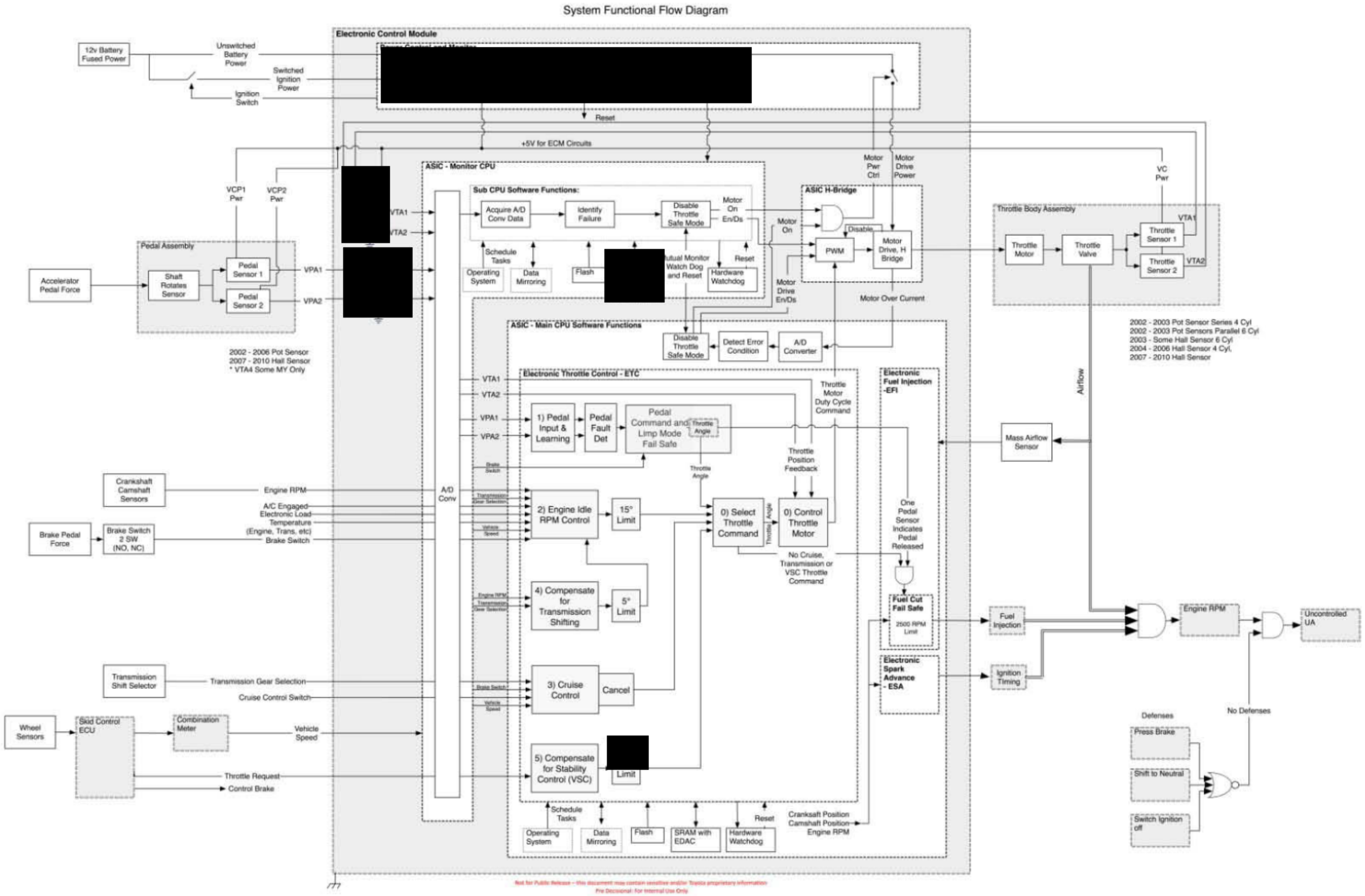


Figure 6.5.1-1. System Redundancy Diagram

There are other postulated failure modes described in Section 6.6 that could result in small throttle openings less than about 5 degrees above normal idle and engine speed less than 2500 rpm. There are also features, not failures, of a normally operating vehicle that open the throttle to maintain proper operation of the vehicle.

1) Air/Fuel Sensor anomalies resulting in hesitation (TMC Field Reports).
2) Transmission shifting and torque converter lockup surges (TMC Field Reports and VOQs).
3) Temperature sensor and engine load sensing anomalies increasing idle engine speed.
4) The engine knock sensor operation could contribute to hesitation when the accelerator pedal is pressed.

6.5.2.1 System Level Functional Fault Tree

The High Level Functional Fault Tree shown in Figure 6.5.2.1-1 shows the combinatorial logic and the system level fail-safe features that must fail for an electronics failure to unintentionally open the throttle a significant amount.

The Functional Fault Tree, Figure 6.5.2.2-2, shows how functional failures and failure causes, captured in the Failure fishbone Appendix B, can combine and result in unintended throttle openings. Hardware and software failure modes and potential environmental causes are captured on the fishbone chart described in Section 6.6. The fishbone organizes failure causes along a functional hierarchy, but without the combinatorial logic necessary to create a UA.

The Functional Fault Tree's high level branches contain the system level fail-safe features with lower level branches organized along the functional architecture of the ETCS-i described in Section 6.6. Figure 6.5.2.2-2 shows the Functional Fault Tree with lower level sensor and actuator fail-safe features and DTCs that flow into the six major functions of the ETCS-i.

System level fail-safe modes control engine speed and power using diverse sensors from the normal throttle position sensors and diverse fuel injection and ignition controls as actuators. Diverse sensors and actuators from the nominal throttle control components can provide defenses against failures potentially escaping the analytical design efforts or lower level DTC detectors.

The right hand side of Figure 6.5.2.2-2 captures conditions where the system level fuel cut fail-safe mode protects the vehicle when the accelerator pedal is released. The “and” gate combines a large anomalous throttle command that escaped detection with the non functioning idle speed fuel cut fail-safe in order to create an event with engine speed higher than 2500 rpm. Barring a software fault described below, the Main CPU will cut the fuel at engine speeds of 2500 rpm regardless what created the throttle command. This fuel cut strategy can protect the vehicle from mechanical throttle valve failures as shown on the left input to the Function 0 “or” gate selecting anomalous throttle commands. Even if the throttle butterfly valve would lose its shape and allow a large amount of air to flow, engine speed would be controlled. As shown in Figure 6.5.2.2-2, Idle Speed Fuel Cut Fail-Safe Mode, can also control electronics failures escaping detection by lower level DTCs. Idle speed fuel cut can control electronics failures originating in the throttle control and idle speed ETCS-i functions creating a throttle command.

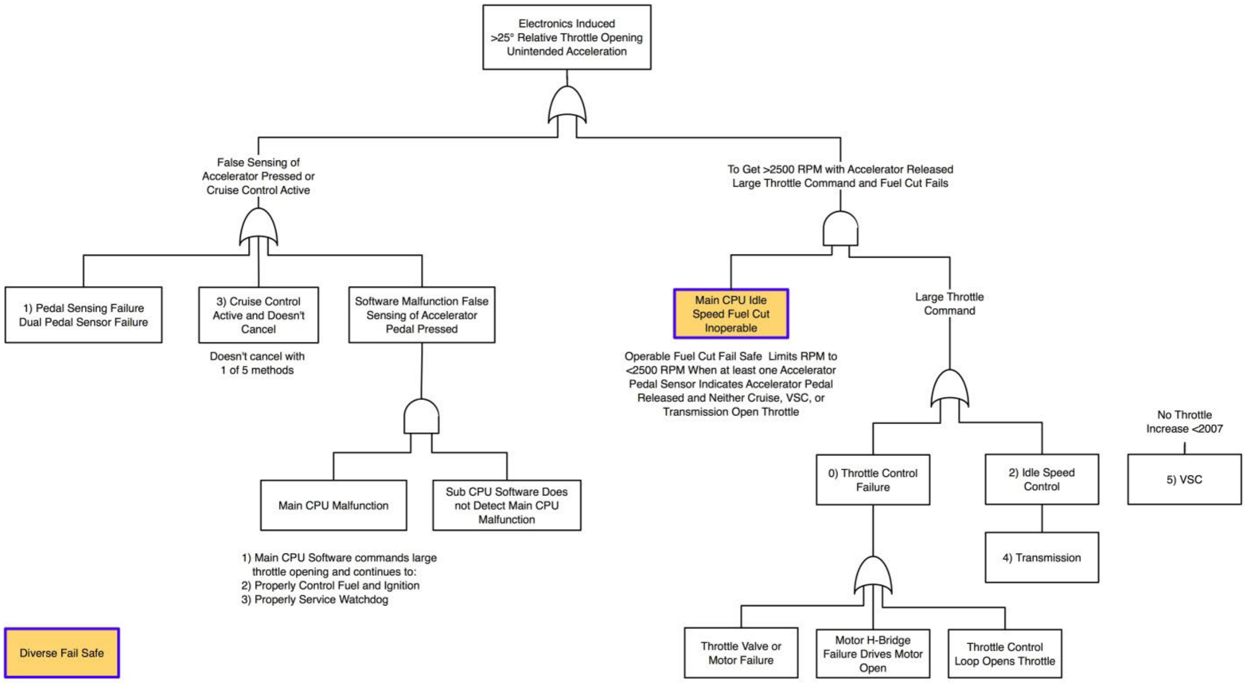


Figure 6.5.2.1-1. High Level Functional Fault Tree

Failures appearing as a valid pedal sensor signal to the Main CPU indicate the accelerator pedal is off idle or is pressed. These kind of functional failures are shown as the left branch of the functional fault tree on the left side of Figure 6.5.2.2-2.

To open the throttle unintentionally without detection, the design of the system requires the functional failure of the two VPA1 and VPA2 accelerator pedal sensor signals to mimic a valid signal, or a software fault indicating that the pedal is pressed. Figure 6.5.2.2-2 includes the lower level branches of the fault tree showing the functional component failures and DTCs serving to identify failures with accelerator pedal sensor components.

Comparing two sensors against each other can protect against failures as long as the failures do not corrupt both the sensors with valid voltages. The selection of VPA1 and VPA2 with an offset serves to protect the system from potential common mode failure causes that may affect both sensors in a way that they may mimic a valid signal. Section 6.6.2 describes accelerator pedal failure modes and the difficulty of detecting such failure modes engineered to mimic valid sensor signals.

The left side of the Functional Fault Tree also identifies the extent of the software failure mode that must occur in both the Main and Sub-CPUs to unilaterally cause UA. These failure paths within a single CPU were not found in the software analysis performed to date. Failures in both CPUs that would allow one software failure to go undetected were also not found.

6.5.2.2 System Level Failure Responses

Figure 6.5.2.2-1 shows the relationship between throttle function control authority in green, the extent each function might open the throttle should the function fail in red along with any software hard limits as a red line. Layered autonomous failure responses are shown in green and driver mitigation options shown in blue. The range of throttle angles where the ability of brakes to slow the vehicle at >0.25 g even with depleted vacuum is shown in orange at angles <35 degrees (absolute). Figure 6.5.2.2-1 shows that throttle system failures shown in red are restricted to levels significantly below the ability of brakes to slow the vehicle at 0.25 g by the built in multilayered fail-safe defenses. Postulated accelerator pedal dual failure scenarios resulting in throttle openings are shown in purple.

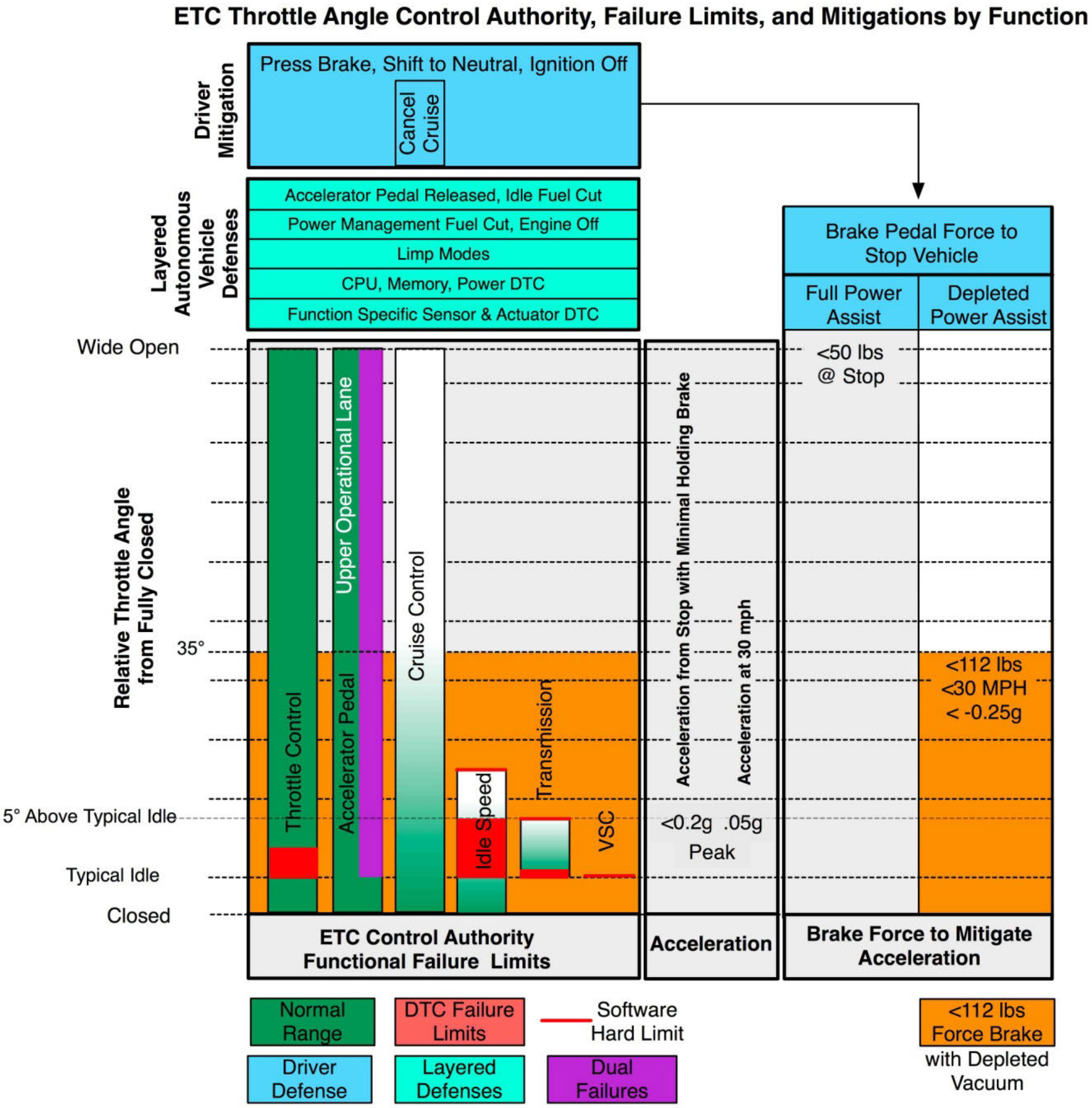

ETC Throttle Angle Control Authority, Failure Limits, and Mitigations by Function
Driver Mitigation
Press Brake, Shift to Neutral, Ignition Off
Cancel Cruise
Layered Autonomous Vehicle Defenses
Accelerator Pedal Released, Idle Fuel Cut
Power Management Fuel Cut, Engine Off
Limp Modes
CPU, Memory, Power DTC
Function Specific Sensor & Actuator DTC
Brake Pedal Force to Stop Vehicle
Full Power Assist
Depleted Power Assist
Wide Open
Relative Throttle Angle from Fully Closed
35°
5° Above Typical Idle
Typical Idle
Closed
Throttle Control
Accelerator Pedal
Upper Operational Lane
Cruise Control
Idle Speed
Transmission
VSC
Acceleration from Stop with Minimal Holding Brake
Acceleration at 30 mph
<0.2g .05g
Peak
<50 lbs @ Stop
<112 lbs
<30 MPH
< -0.25g
ETC Control Authority Functional Failure Limits
Acceleration
Brake Force to Mitigate Acceleration
Normal Range
DTC Failure Limits
Software Hard Limit
Driver Defense
Layered Defenses
Dual Failures
<112 lbs Force Brake
with Depleted Vacuum

Figure 6.5.2.2-1. ETCS-i Throttle Angle Control Authority, Failure Limits, and Mitigation by Function

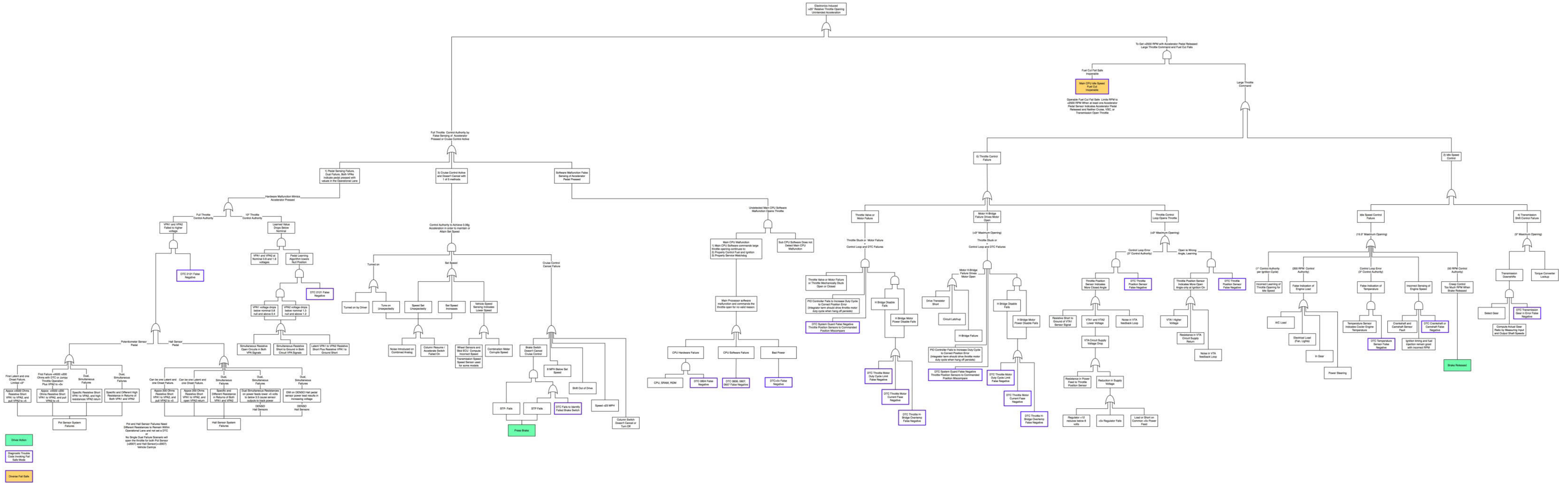

Electronics Induced >25° Relative Throttle Opening Unintended Acceleration
Full Throttle Control Authority by False Sensing of Accelerator Pressed or Cruise Control Active
1) Pedal Sensing Failure, Dual Failure, Both VPAs indicate pedal pressed with values in the Operational Lane
3) Cruise Control Active and Doesn't Cancel with 1 of 5 methods
Software Malfunction False Sensing of Accelerator Pedal Pressed
Hardware Malfunction Mimics Accelerator Pressed
Full Throttle Control Authority
10° Throttle Control Authority
VPA1 and VPA2 Failed to higher voltage
DTC 2121 False Negative
Learned Value Drops Below Nominal
VPA1 and VPA2 at Nominal 0.8 and 1.6 voltages
Pedal Learning Algorithm lowers Null Position
DTC 2121 False Negative
VPA1 voltage drops below nominal 0.8 null and above 0.4
VPA2 voltage drops below nominal 1.3 null and above 1.2
Simultaneous Resistive Open Circuits in Both VPA Signals
Simultaneous Resistive Short to Ground in Both Circuit VPA Signals
Latent VPA1 to VPA2 Resistive Short Plus Resistive VPA1 to Ground Short
Potentiometer Sensor Pedal
Hall Sensor Pedal
First Latent and one Onset Failure. Limited <3°
First Failure <4500 >200 Ohms with DTC or Jumpy Throttle Operation Plus VPA2 to +5v
Dual, Simultaneous Failures
Dual, Simultaneous Failures
Appox >4500 Ohms Resistive Short VPA1 to VPA2, and pull VPA2 to +5
Appox <4500 >200 Ohms Resistive Short VPA1 to VPA2, and pull VPA2 to +5
Specific Resistive Short VPA1 to VPA2, and high resistances VPA2 return
Specific and Different High Resistance in Returns of Both VPA1 and VPA2
Pot Sensor System Failures
Can be one Latent and one Onset Failure.
Can be one Latent and one Onset Failure.
Dual, Simultaneous Failures
Dual, Simultaneous Failures
Dual, Simultaneous Failures
Appox 200 Ohms Resistive Short VPA1 to VPA2, and pull VPA2 to +5
Appox 200 Ohms Resistive Short VPA1 to VPA2, and open VPA2 return
Specific and Different Resistance in Returns of Both VPA1 and VPA2
Dual Simultaneous Resistances on power feeds lower +5 volts to below 3.3 cause sensor outputs to track power
EMI on DENSO Hall pedal sensor power lead results in increasing voltage
DENSO Hall Sensors
DENSO Hall Sensors
Hall Sensor System Failures
Pot and Hall Sensor Failures Need Different Resistances to Remain Within Operational Lane and not set a DTC
or
No Single Dual Failure Scenario will open the throttle for both Pot Sensor (<2007) and Hall Sensor(>=2007) Vehicle Camrys
Driver Action
Diagnostic Trouble Code Invoking Fail Safe Mode
Diverse Fail Safe
Control Authority to Achieve 0.06g Acceleration in order to maintain or Attain Set Speed
Turned on
Set Speed
Cruise Control Cancel Failure
Turned on by Driver
Turns on Unexpectedly
Speed Set Unexpectedly
Set Speed Increases
Vehicle Speed Sensing Indicates Lower Speed
Noise Introduced on Combined Analog
Column Resume / Accelerate Switch Failed On
Wheel Sensors and Skid ECU Compute Incorrect Speed
Transmission Speed Speed Sensor used for some models
Combination Meter Corrupts Speed
Brake Switch Doesn't Cancel Cruise Control
8 MPH Below Set Speed
Shift Out of Drive
Speed <23 MPH
Column Switch Doesn't Cancel or Turn Off
STP- Fails
STP Fails
DTC Fails to Identify Failed Brake Switch
Press Brake
Undetected Main CPU Software Malfunction Opens Throttle
Main CPU Malfunction
1) Main CPU Software commands large throttle opening continues to:
2) Properly Control Fuel and Ignition
3) Properly Service Watchdog
Sub CPU Software Does not Detect Main CPU Malfunction
Main Processor software malfunction and commands the throttle open for no valid reason.
CPU Hardware Failure
CPU Software Failure
Bad Power
CPU, SRAM, ROM
DTC 0604 False Negative
DTC 0606, 0607, 0657 False Negative
DTC+5v False Negative
To Get >2500 RPM with Accelerator Pedal Released: Large Throttle Command and Fuel Cut Fails
Fuel Cut Fail Safe Inoperable
Main CPU Idle Speed Fuel Cut Inoperable
Operable Fuel Cut Fail Safe Limits RPM to <2500 RPM When at least one Accelerator Pedal Sensor Indicates Accelerator Pedal Released and Neither Cruise, VSC, or Transmission Open Throttle
Large Throttle Command
0) Throttle Control Failure
2) Idle Speed Control
Throttle Valve or Motor Failure
Throttle Stuck or Motor Failure + Control Loop and DTC Failures
Throttle Valve or Motor Failure or Throttle Mechanically Stuck Open or Closed
PID Controller Fails to Increase Duty Cycle to Correct Position Error (Integrator term should drive throttle motor duty cycle when hang off persists)
DTC System Guard False Negative Throttle Position Sensors to Commanded Position Miscompare
H Bridge Disable Fails
H Bridge Motor Power Disable Fails
DTC Throttle Motor Duty Cycle Limit False Negative
DTC Throttle Motor Current Fase Negative
DTC Throttle H-Bridge Overtemp False Negative
Motor H-Bridge Failure Drives Motor Open
(<3° Maximum Opening)
Throttle Stuck or + Control Loop and DTC Failures
Motor H-Bridge Failure Drives Motor Open
Drive Transistor Short
Circuit Latchup
H-Bridge Failure
PID Controller Fails to Increase Duty Cycle to Correct Position Error (Integrator term should drive throttle motor duty cycle when hang off persists)
DTC System Guard False Negative Throttle Position Sensors to Commanded Position Miscompare
H Bridge Disable Fails
H Bridge Motor Power Disable Fails
DTC Throttle Motor Duty Cycle Limit False Negative
DTC Throttle Motor Current Fase Negative
DTC Throttle H-Bridge Overtemp False Negative
Throttle Control Loop Opens Throttle
(<3° Maximum Opening)
Control Loop Error (3° Control Authority)
Open to Wrong Angle, Learning
Throttle Position Sensor Indicates More Closed Angle
DTC Throttle Position Sensor False Negative
Throttle Position Sensor Indicates More Open Angle only at Ignition On
DTC Throttle Position Sensor False Negative
Resistive Short to Ground of VTA1 Sensor Signal
VTA1 and VTA2 Lower Voltage
Noise in VTA feedback Loop
VTA Circuit Supply Voltage Drop
Resistance in Power Feed to Throttle Position Sensor
Reduction in Supply Voltage
Regulator +12 reduces below 8 volts
+5v Regulator Fails
Load or Short on Common +5v Power Feed
VTA1 Higher Voltage
Resistance in VTA Circuit Supply Return
Noise in VTA feedback Loop
Idle Speed Control Failure
(15.5° Maximum Opening)
(1° Control Authority per Ignition Cycle)
(200 RPM Control Authority)
Control Loop Error (3° Control Authority)
(50 RPM Control Authority)
Incorrect Learning of Throttle Opening for Idle Speed
False Indication of Engine Load
False Indication of Temperature
Incorrect Sensing of Engine Speed
Creep Control Too Much RPM When Brake Released
A/C Load
Electrical Load (Fan, Lights)
In Gear
Power Steering
Temperature Sensor Indicates Cooler Engine Temperature
DTC Temperature Sensor False Negative
Crankshaft and Camshaft Sensor Fault
DTC Crankshaft or Camshaft False Negative
Ignition timing and fuel injection remain good with incorrect RPM
Brake Released
4) Transmission Shift Control Failure
(5° Maximum Opening)
Transmission Downshifts
Torque Converter Lockup
Select Gear
DTC Transmission Gear in Error False Negative
Compute Actual Gear Ratio by Measuring Input and Output Shaft Speeds

Figure 6.5.2.2-2. System Level Functional Fault Tree

Table 6.5.2.2-1 summarizes postulated failures of the major electronics components along functional areas, how they may be created, how they are detected, the applicable failure response, whether they have been observed under normal operations and any system level protection. Five of the 6 questions posed by NHTSA are summarized in the numbered columns.

The column title "2 Failure Conditions and Failure symptoms found in Normal Operating Environment" identifies whether the postulated failure has been observed in VOQ data, warranty records, TMC Field Reports, and whether NESC testing was able to duplicate the failure and the system response.

The two pink rows identify the failure modes capable of opening the throttle more than 5 degrees under carefully engineered failure modes not evident in the normal operating environment data observed to date. ISC engine speed changes resulting from failures of sensor inputs are also limited to less than 5 degrees even though the maximum software limit is 15 degrees.

Table 6.5.2.2-1. Summary ETCS-i Failure Modes, Evidence, and Responses

Note 1: Column 2 refers to failures that resulted in a DTC for that function or a test. Does not refer to a UA

Functional Area	**Electronics Component**	**1) Conditions necessary for Failure to Occur, Failure Mode**	**2) Failure Conditions and Failure symptoms found in Real World?** Note 1	**3) Physical or Electronic Evidence, Failure Detection**	**4) Range of throttle opening**	**5) Failure Effect Braking**	**System Failure Response, Applicable Safe Modes**	**System Level Protection**
Throttle Control	Throttle Position Sensors	Position Sensor Fail High, Low, Intermediate values. Compromised power feed or ground to both sensors.	Single Throttle Sensor failures in Warranty data, NESC Engineered Test	DTC for sensors not within the valid range. DTC Position does not match commanded	Small openings <3 to 5 between normal sensor values and DTC limit	None	#3 Disable Throttle Motor Limp Mode, Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6 5 off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal If RPM > limit after motor disabled, vehicle is shut off.	Idle Mode Fuel Cut, #4 Fuel Cut Limits < 2500 rpm when accelerator pedal released
		Incorrect Learning of Fully closed Position, Sensor voltage lower	No evidence in warranty data, NESC Engineered Test		Small openings <3 between normal sensor values and DTC limit	None		
	Throttle Motor	Motor shorted to Power or Ground, Open, H-Bridge Fail, Latch-up or Transistor Short (Throttle Valve Stuck for mechanical failure)	ECM and Throttle Body failures in Warranty data, NESC Engineered Test	DTC High current, duty Cycle, or temperature	Transitory small openings until DTC activates fail-safe mode <0.5 sec	None		
Idle Speed Control	Idle Speed Sensors	Temperature Sensor Fail High, Low, Intermediate values, Engine, Coolant, Power Steering, Transmission	Sensor failures in Warranty data, NESC Engineered Test	DTC for Sensors not within operational zone	Small openings <3 to 5 between normal sensor values and DTC limit	None		
		Incorrect Sensing of Engine Load, Gear, Power Steering, A/C, Electric Load, Engine Speed	Sensor failures in Warranty data, NESC Engineered Test	DTC for Sensors not within operational zone, Engine Stall	Small openings <3 to 5 between normal sensor values and DTC limit	None		
		Incorrect Learning of Throttle angle for Idle Speed	No evidence in warranty data,, NESC Observed in Test		Small openings <3 to 5 between normal sensor values and DTC limit	None		
	Engine Sensors	Air/Fuel, O2, Knock Sensors modulate air fuel or timing resulting in surging	TQCN	DTC for Sensors not within operational zone	Small openings <3 to 5 between normal sensor values and DTC limit	None	Open Loop Fuel Trim	
Transmission Shifting	Transmission Sensors	Transmission Shifting, Torque Converter Lockup Throttle Modulation	TQCN, NESC Observed in Test	DTC when Selected Gear doesn't match sensed gear ratio	Small openings <5	None	DTC results in selection up one gear	
Pedal Command	Pedal Sensors	Position Sensor Fail High, Low, Intermediate values	Pedal sensor failures in Warranty data, NESC Engineered Test	DTC for high, low and outside lane. None, if Pedal sensors fail within operational lane DTC	(Throttle does not open with a single failure)	-	Limp Home Mode #1, Throttle control limited to 15 relative opening above idle, by remaining sensor. If neither Pedal Sensor operable then Idle only. Under certain conditions on Potentiometer Sensor Vehicles, Limp mode throttle is not limited and can jump depending how fast accelerator pedal is pressed[16]	
		Incorrect Learned Value, Dual failures to specific voltages that result in voltages within operational lane	No evidence in warranty data,, NESC Engineered Test	Engineered Fault in operational lane Valid pedal signal escapes detection, no DTC. Electrical Failures should leave trace.	Small openings < 10 max between normal sensor values and DTC limit	-	None, Dual failures look like a valid pedal signal cannot be detected, 10 max opening	

[16] See section 6.6.2.3 for a description of the Limp Home Mode and the particular ignition key cycle and pedal application conditions where the throttle opening may not be limited after DTC 2121 is detected.

Functional Area	**Electronics Component**	**1) Conditions necessary for Failure to Occur, Failure Mode**	**2) Failure Conditions and Failure symptoms found in Real World?** Note 1	**3) Physical or Electronic Evidence, Failure Detection**	**4) Range of throttle opening**	**5) Failure Effect Braking**	**System Failure Response, Applicable Safe Modes**	**System Level Protection**
		Dual failures that result in voltages within operational lane	No signs of dual resistive failures, NESC Engineered Test	Engineered Fault in operational lane Valid pedal signal escapes detection, no DTC. Electrical Failures should leave trace.	Openings up to wide open throttle conceptually possible although not found in real world	Functional Effect >35 , could deplete vacuum brake assist if brakes pumped	None, Dual failures that emulate or look like a valid pedal signal cannot be detected	None possible for multiple failures that look like a valid pedal signal
Cruise Control	Cruise Control	Failure of Steering Column Switches or ECM input circuit	Cruise control switch failures in Warranty data, Engineered Test	Short to power, ground, open disables function	Small throttle openings to maintain 0.06g acceleration to set speed	None	Specific ordering for activation, Short to ground is off	Driver can activate, Brake Switch, or 9 mph slow down cancels Cruise, or cancel cruise, or shift to neutral
		Failed Brake Switch	No dual brake switch failure found in warranty data, Engineered Test	DTC when both Brake Switch poles do not agree. Cannot switch into Gear Cruise will not cancel when brake pressed	Large throttle openings when brake is pressed to slow vehicle and vehicle attempts to accelerate at 0.06g	None	Car accelerates at 0.06g to maintain set speed. Cancel or Off necessary to disable Cruise Control	
		Vehicle Speed sensor indicates lower speed	Speed sensor failures in Warranty data	DTC for Speed Sensor, Skid ECM, Combination Meter	Small throttle openings to maintain 0.06g acceleration to set speed	None	Sensor ignored, Cruise Control Cancel at 9 mph reduction	
Throttle Control, Computer	Main CPU	Faulty Power, Memory Failure	ECM failures in Warranty data, NESC Engineered Test	DTC for bad Power, Memory fault, Consistent Data	None	-	Engine Turned Off	Engine Turned Off #6
	Sub-CPU	Faulty Power, Memory Failure	ECM failures in Warranty data, NESC Engineered Test	DTC for bad Power, Memory fault, Consistent Data	None	-		
	Main CPU Software	Software unilaterally opens throttle with Accelerator released, Idle Fuel Cut not active, Watchdog serviced, no EDAC error, Sub-CPU does not Detect Failure	No, Cannot engineer a test. No place found in software where a single memory/variable corruption results in a UA	Theoretical Fault Escapes Detection	Openings up to wide open throttle conceptualized although not found in real world	Functional Effect >35 , could deplete vacuum brake assist if brakes pumped	Engineered Fault Escapes Detection	None possible, malfunctioning computer opens throttle appears normal without DTC, watchdog timeout, Limp Mode or other errors

6.5.2.3 System Fail-safe Modes

The ETCS-i employs several fail-safe modes that balance the hazards of stranding the vehicle and allowing the vehicle to move. Fail-safe modes safe the vehicle by controlling throttle valve position and taking action commensurate with the affected function. If the failure involves one of the pedal sensors, the throttle valve is operated over a limited angle based on the remaining sensor to allow the driver to limp home or pull off to the side of the road. If the failure involves the throttle sensors or the motor, the throttle valve is returned to its spring loaded detent position with engine power controlled via fuel injection and spark based on the pedal sensors. If the failure involves the CPU or the throttle valve cannot be controlled or returned to its spring loaded detent position, resulting in a high mass air flow then the engine is turned off.

Fail-safe modes are summarized Table 6.5.2.2-2. Each fail-safe mode provides a function and employs an approach for performing that function.

Table 6.5.2.2-2. Fail-safe Modes

	Limp Modes			Fuel Cut	Vehicle Off
Fail Safe Modes	**1** **Limp Home Mode (Pedal Failure, Throttle Operable)**	**2** **Engine at Idle (Neither Pedal Sensor Operable, Throttle at Idle)**	**3** **Disable Throttle Motor (Throttle sensor or motor failure, Throttle at spring detent)**	**4** **Idle Mode Fuel Cut (Normal Operation, Accelerator Pedal Released)**	**5** **Engine Turned Off (CPU failure or Throttle stuck with high air flow, Fuel and Ignition Cut off)**
Function and Strategy	Allows vehicle to travel under reduced engine power. Working pedal sensor used to control Throttle but limited to 15 degrees maximum opening depending on the engine. Under certain conditions on Potentiometer Sensor Vehicles, Limp mode throttle is not limited and can jump depending how fast accelerator pedal is pressed [17]	Car limited to Idle. Throttle controlled to maintain idle speed.	Allows vehicle to idle and move at slightly above idle power. Throttle motor depowered and H-Bridge disabled Throttle mechanically held at 6.5 degrees spring loaded detent. Control engine speed via Power Management Fuel Cut based on pedal position	Limits maximum engine speed with Foot-off pedal. Control engine speed by Fuel cut off at 2500 rpms, fuel turned on at 1100 rpm Power Management Fuel Cut	Completely shuts off the vehicle

[17] See section 6.6.2.3 for a description of the Limp Mode and the particular ignition key cycle and pedal application conditions where the throttle opening may not be limited after DTC 2121 is detected.

	Limp Modes			Fuel Cut	Vehicle Off
Fail Safe Modes	**1** **Limp Home Mode (Pedal Failure, Throttle Operable)**	**2** **Engine at Idle (Neither Pedal Sensor Operable, Throttle at Idle)**	**3** **Disable Throttle Motor (Throttle sensor or motor failure, Throttle at spring detent)**	**4** **Idle Mode Fuel Cut (Normal Operation, Accelerator Pedal Released)**	**5** **Engine Turned Off (CPU failure or Throttle stuck with high air flow, Fuel and Ignition Cut off)**
Initiating Failure Causes	VPA1 or VPA2 failed high or low, or do not agree (DTCs). VPA1 fail low and VPA2 fail high. (DTC 2120, 2121, 2122, 2123, 2125, 2127, 2128) (DTC 1120 and 1121 for MY 2002)	Both pedal sensors failed. VPA1 and VPA2 both fail high or low. VP1 fail high, VPA2 fail low. (DTC 2121, 2138) (DTC 1120 for MY 2002)	VTA1 and/or VTA2 failed high or low, or do not agree. High Motor Current or temperature, Throttle stuck open or closed (DTC 0120, 0121, 0122, 0123, 0220, 0222, 0223, 2135)	Accelerator Released and High engine speed >2500. Caused by: Throttle valve allows airflow, Electronics failures drives motor open with throttle sensors at idle, normal throttle motor current	CPU Failures, Load the +5V (DTC 0604, 0606, 0607, 0657) VTA1 and VTA2 indicate throttle is stuck open or closed. Throttle valve jammed open, Throttle sensors indicate position in error, High Motor Duty Cycle High Motor Current (DTC 2102, 2103, 2111, 2112, 2118, 2119)
Brake Pedal	Closes Throttle to Idle Position				

6.5.3 Failure Mitigation

The following sections describe each of the fail-safe modes summarized in Table 6.5.2.2-2.

6.5.3.1 Limp Home Mode, Throttle Valve Control Limited

Limp home mode provides a mechanism to operate the vehicle at reduced engine power when a failure is detected in one of the two pedal sensors. The remaining sensor is used to control the throttle to a maximum opening limited to about 15 degrees. This mode is summarized in column 1.

The limp home mode also provides a mechanism to close the throttle valve when the brake pedal is pressed activating the brake switch. If one of the VPAs is sensed as failed and the other is used to control the throttle in limp home mode commanding the throttle to open, the ETCS-i automatically closes the throttle when the brake is pressed. Closing the throttle valve in response to the brake serves to reduce vehicle power should the second VPA fail in a manner that results in an opening of the throttle.

O-2. *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 defense against unintended engine power whether caused by electronic, software, mechanical failures.*

Under a particular set of VPA1 to VPA2 resistive shorts[18], the ETCS-i generates DTC 2121, the MIL is illuminated, and the fail-safe limp home mode is entered with its limited maximum throttle opening and throttle return to idle position when the brake pedal is pressed. However, with the resistive short, the fail-safe limp home performance was found to change after the ignition is cycled resulting in functional implications.

For MY 2006 and earlier, after a key cycle with the failure in place, when the accelerator pedal is pushed quickly, i.e., less than 0.5 seconds through the first 0.5 inch of pedal travel, then the vehicle remains in limp home mode with all of the fail-safe features described above. However, if the accelerator pedal is pushed slowly, i.e., more than 0.5 seconds through the first 0.5 inch of pedal travel, the throttle valve may jump up to a 14 degrees relative throttle valve opening and can be completely opened if the accelerator pedal is fully depressed. In addition, if the accelerator remains depressed, the throttle does not return to idle when the brake is simultaneously pressed. If the accelerator pedal is released the throttle will close smoothly. Functionally, in the presence of this particular resistive failure between VPA1 and VPA2 the smooth 15 degrees maximum angle throttle opening of the fail-safe limp home mode is lost after a key cycle and replaced by jumpy throttle performance characterized by a hesitation followed by throttle opening jumps and return to idle when the pedal is released.

If the DTC 2121 is cleared and the MIL is turned off via an OBD II clear code command or via a battery power disconnect, neither the DTC 2121 nor the MIL will re-illuminate for this range of resistive short conditions. Even though the DTC was cleared and the MIL might not be on, the operation of the system with the resistive short in place remains the same as described above. Depending on how the pedal is pressed, the system can either enter the fail-safe limp home mode or the alternate mode with the potential for the throttle to jump depending on how the pedal is pressed, or if the vehicle is started with the pedal pressed.

Similar performance was observed on MY 2007, but without the jumpy throttle response. Specifically, when the accelerator pedal is pushed quickly, the vehicle remains in limp home

[18] See Section 6.6.2 for quantification of the partial resistive short and the applicable pedal sensor implementation, (potentiometer, CTS or Denso Hall sensor)

mode with all of the fail-safe features described above. However, if the accelerator pedal is pushed slowly, the throttle valve can fully open without a jumpy response.

6.5.3.2 Engine at Idle

The engine at idle mode allows the engine to run with throttle control limited to idle. The electronic throttle will compensate for engine load changes including air conditioning and transmission loads. The vehicle can be operated at idle speed, but no appreciable road speed can be achieved. This mode is entered when the ETCS-i cannot validate either of the pedal position sensors. The throttle control function operates properly and therefore can be used to allow the vehicle to move and power assisted braking and steering is maintained.

6.5.3.3 Disable Throttle Motor, Throttle held at 6.5 Degrees Spring Loaded Detent

When the throttle valve position does not match the commanded position, or the motor duty-cycle is too high, or the motor current is high, or the H-Bridge temperature is too high, a failure in the throttle motor and or positioning is presumed and power is removed from the throttle motor. The disable throttle motor safe mode removes power from the throttle motor through two methods. The Main CPU and Sub-CPU can power off the power feed to the H-Bridge and disable both the high side and low side transistors of the H-Bridge.

This mode is entered in response to a failure of the throttle position sensors that causes the actual position of the throttle to be uncertain without indication of high duty cycle or high current. When the throttle position cannot be validated the ETCS-i can no longer reliably control the throttle position, the throttle motor is disabled.

After the throttle motor is disabled the throttle valve returns to its spring loaded detent position located 6.5 degrees from fully closed. At such a throttle opening the engine can be operated at engine speeds above normal idle and with some additional power, but at low speeds only. To control the engine speed and power, a fuel cut function modulates fuel flow and ignition timing based on pedal position.

6.5.3.4 Idle Mode Fuel Cut, Engine Speed limited <2500 rpm

Idle Mode Fuel Cut functionally provides an engine speed and power limiter under accelerator pedal not pressed conditions, which is determined if at least one of the two pedal sensors indicates it is at its idle position. When the throttle motor and its sensors are functional, ISC should be keeping the idle engine speed under 2500 rpms. If the engine speed increase above 2500 rpm, then some undetected failure could result in uncommanded throttle openings affecting engine speed. The idle mode fuel cut provides an overall safe mode umbrella for failures escaping detection or control and controls the resulting increased engine speed when the accelerator is sensed as not pressed.

6.5.3.5 Engine Off Fail-Safe

The engine is stopped when the CPUs can no longer control the throttle opening or air flow. When it is not safe to continue operating the engine fuel and ignition are cut to stop the engine. This can be caused by CPU watchdog failures, or low voltage on the +5V and as an uncontrollable throttle valve or a high unintended mass airflow.

6.6 Functional Areas with Functional Block Diagrams, Test Scenarios, and Test Results

An Ishikawa (fishbone) diagram, Figure 6.6-1, lists in functional hierarchy potential failure causes of UA postulated based on the NESC team's assessment. Each postulated failure cause was dispositioned through analysis or test and the closure of each of the elements of the fishbone was documented in a table. The analysis and disposition of fishbone elements is contained in Appendix B.

The fishbone for this investigation was developed to address functional failures and, consequently, does not devolve to the part level. It is configured into 9 major areas: Throttle Function, Pedal Function, Cruise Control Function, Idle Speed Control Function, Transmission Shifting and VSC Function, Software, Environmental Effects, Power, and Mechanical Effects.

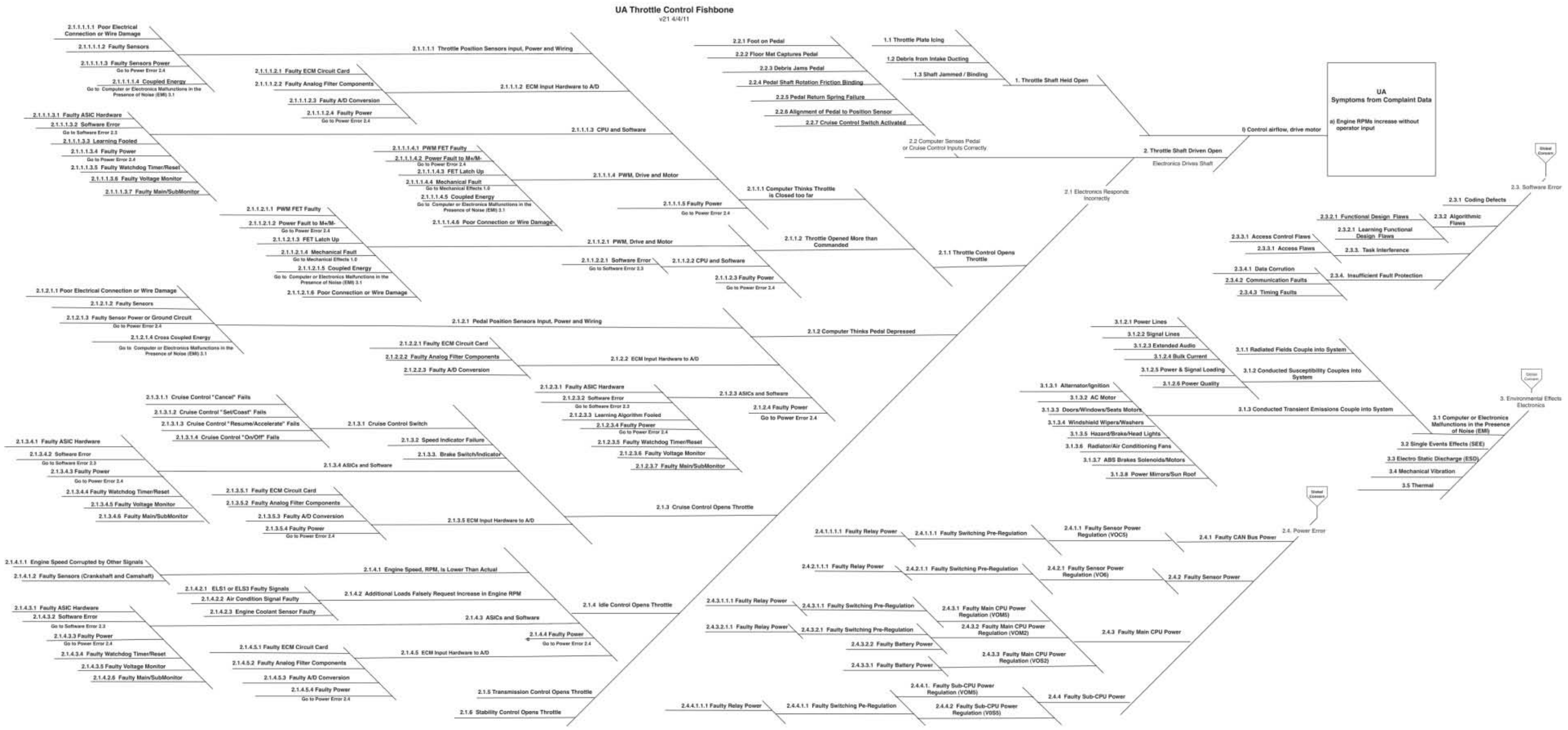

UA Throttle Control Fishbone
v21 4/4/11
2.1.1.1.1.1 Poor Electrical Connection or Wire Damage
2.1.1.1.1.2 Faulty Sensors
2.1.1.1.1.3 Faulty Sensors Power
Go to Power Error 2.4
2.1.1.1.1.4 Coupled Energy
Go to Computer or Electronics Malfunctions in the Presence of Noise (EMI) 3.1
2.1.1.1.1 Throttle Position Sensors input, Power and Wiring
2.1.1.1.2.1 Faulty ECM Circuit Card
2.1.1.1.2.2 Faulty Analog Filter Components
2.1.1.1.2.3 Faulty A/D Conversion
2.1.1.1.2.4 Faulty Power
Go to Power Error 2.4
2.1.1.1.2 ECM Input Hardware to A/D
2.1.1.1.3.1 Faulty ASIC Hardware
2.1.1.1.3.2 Software Error
Go to Software Error 2.3
2.1.1.1.3.3 Learning Fooled
2.1.1.1.3.4 Faulty Power
Go to Power Error 2.4
2.1.1.1.3.5 Faulty Watchdog Timer/Reset
2.1.1.1.3.6 Faulty Voltage Monitor
2.1.1.1.3.7 Faulty Main/SubMonitor
2.1.1.1.3 CPU and Software
2.1.1.1.4.1 PWM FET Faulty
2.1.1.1.4.2 Power Fault to M+/M-
Go to Power Error 2.4
2.1.1.1.4.3 FET Latch Up
2.1.1.1.4.4 Mechanical Fault
Go to Mechanical Effects 1.0
2.1.1.1.4.5 Coupled Energy
Go to Computer or Electronics Malfunctions in the Presence of Noise (EMI) 3.1
2.1.1.1.4.6 Poor Connection or Wire Damage
2.1.1.1.4 PWM, Drive and Motor
2.1.1.1.5 Faulty Power
Go to Power Error 2.4
2.1.1.1 Computer Thinks Throttle is Closed too far
2.1.1.2.1.1 PWM FET Faulty
2.1.1.2.1.2 Power Fault to M+/M-
Go to Power Error 2.4
2.1.1.2.1.3 FET Latch Up
2.1.1.2.1.4 Mechanical Fault
Go to Mechanical Effects 1.0
2.1.1.2.1.5 Coupled Energy
Go to Computer or Electronics Malfunctions in the Presence of Noise (EMI) 3.1
2.1.1.2.1.6 Poor Connection or Wire Damage
2.1.1.2.1 PWM, Drive and Motor
2.1.1.2.2.1 Software Error
Go to Software Error 2.3
2.1.1.2.2 CPU and Software
2.1.1.2.3 Faulty Power
Go to Power Error 2.4
2.1.1.2 Throttle Opened More than Commanded
2.1.1 Throttle Control Opens Throttle
2.1.2.1.1 Poor Electrical Connection or Wire Damage
2.1.2.1.2 Faulty Sensors
2.1.2.1.3 Faulty Sensor Power or Ground Circuit
Go to Power Error 2.4
2.1.2.1.4 Cross Coupled Energy
Go to Computer or Electronics Malfunctions in the Presence of Noise (EMI) 3.1
2.1.2.1 Pedal Position Sensors Input, Power and Wiring
2.1.2.2.1 Faulty ECM Circuit Card
2.1.2.2.2 Faulty Analog Filter Components
2.1.2.2.3 Faulty A/D Conversion
2.1.2.2 ECM Input Hardware to A/D
2.1.2.3.1 Faulty ASIC Hardware
2.1.2.3.2 Software Error
Go to Software Error 2.3
2.1.2.3.3 Learning Algorithm Fooled
2.1.2.3.4 Faulty Power
Go to Power Error 2.4
2.1.2.3.5 Faulty Watchdog Timer/Reset
2.1.2.3.6 Faulty Voltage Monitor
2.1.2.3.7 Faulty Main/SubMonitor
2.1.2.3 ASICs and Software
2.1.2.4 Faulty Power
Go to Power Error 2.4
2.1.2 Computer Thinks Pedal Depressed
2.1.3.1.1 Cruise Control "Cancel" Fails
2.1.3.1.2 Cruise Control "Set/Coast" Fails
2.1.3.1.3 Cruise Control "Resume/Accelerate" Fails
2.1.3.1.4 Cruise Control "On/Off" Fails
2.1.3.1 Cruise Control Switch
2.1.3.2 Speed Indicator Failure
2.1.3.3. Brake Switch/Indicator
2.1.3.4.1 Faulty ASIC Hardware
2.1.3.4.2 Software Error
Go to Software Error 2.3
2.1.3.4.3 Faulty Power
Go to Power Error 2.4
2.1.3.4.4 Faulty Watchdog Timer/Reset
2.1.3.4.5 Faulty Voltage Monitor
2.1.3.4.6 Faulty Main/SubMonitor
2.1.3.4 ASICs and Software
2.1.3.5.1 Faulty ECM Circuit Card
2.1.3.5.2 Faulty Analog Filter Components
2.1.3.5.3 Faulty A/D Conversion
2.1.3.5.4 Faulty Power
Go to Power Error 2.4
2.1.3.5 ECM Input Hardware to A/D
2.1.3 Cruise Control Opens Throttle
2.1.4.1.1 Engine Speed Corrupted by Other Signals
2.1.4.1.2 Faulty Sensors (Crankshaft and Camshaft)
2.1.4.1 Engine Speed, RPM, Is Lower Than Actual
2.1.4.2.1 ELS1 or ELS3 Faulty Signals
2.1.4.2.2 Air Condition Signal Faulty
2.1.4.2.3 Engine Coolant Sensor Faulty
2.1.4.2 Additional Loads Falsely Request Increase in Engine RPM
2.1.4.3.1 Faulty ASIC Hardware
2.1.4.3.2 Software Error
Go to Software Error 2.3
2.1.4.3.3 Faulty Power
Go to Power Error 2.4
2.1.4.3.4 Faulty Watchdog Timer/Reset
2.1.4.3.5 Faulty Voltage Monitor
2.1.4.2.6 Faulty Main/SubMonitor
2.1.4.3 ASICs and Software
2.1.4.4 Faulty Power
Go to Power Error 2.4
2.1.4.5.1 Faulty ECM Circuit Card
2.1.4.5.2 Faulty Analog Filter Components
2.1.4.5.3 Faulty A/D Conversion
2.1.4.5.4 Faulty Power
Go to Power Error 2.4
2.1.4.5 ECM Input Hardware to A/D
2.1.4 Idle Control Opens Throttle
2.1.5 Transmission Control Opens Throttle
2.1.6 Stability Control Opens Throttle
2.1 Electronics Responds Incorrectly
2.2.1 Foot on Pedal
2.2.2 Floor Mat Captures Pedal
2.2.3 Debris Jams Pedal
2.2.4 Pedal Shaft Rotation Friction Binding
2.2.5 Pedal Return Spring Failure
2.2.6 Alignment of Pedal to Position Sensor
2.2.7 Cruise Control Switch Activated
2.2 Computer Senses Pedal or Cruise Control Inputs Correctly
1.1 Throttle Plate Icing
1.2 Debris from Intake Ducting
1.3 Shaft Jammed / Binding
1. Throttle Shaft Held Open
2. Throttle Shaft Driven Open
Electronics Drives Shaft
I) Control airflow, drive motor
UA
Symptoms from Complaint Data
a) Engine RPMs increase without operator input
Global Concern
2.3. Software Error
2.3.1 Coding Defects
2.3.2.1 Functional Design Flaws
2.3.2.1 Learning Functional Design Flaws
2.3.2 Algorithmic Flaws
2.3.3.1 Access Control Flaws
2.3.3.1 Access Flaws
2.3.3. Task Interference
2.3.4.1 Data Corrution
2.3.4.2 Communication Faults
2.3.4.3 Timing Faults
2.3.4. Insufficient Fault Protection
3.1.2.1 Power Lines
3.1.2.2 Signal Lines
3.1.2.3 Extended Audio
3.1.2.4 Bulk Current
3.1.2.5 Power & Signal Loading
3.1.2.6 Power Quality
3.1.1 Radiated Fields Couple into System
3.1.2 Conducted Susceptibility Couples into System
3.1.3.1 Alternator/Ignition
3.1.3.2 AC Motor
3.1.3.3 Doors/Windows/Seats Motors
3.1.3.4 Windshield Wipers/Washers
3.1.3.5 Hazard/Brake/Head Lights
3.1.3.6 Radiator/Air Conditioning Fans
3.1.3.7 ABS Brakes Solenoids/Motors
3.1.3.8 Power Mirrors/Sun Roof
3.1.3 Conducted Transient Emissions Couple into System
3. Environmental Effects Electronics
3.1 Computer or Electronics Malfunctions in the Presence of Noise (EMI)
3.2 Single Events Effects (SEE)
3.3 Electro Static Discharge (ESD)
3.4 Mechanical Vibration
3.5 Thermal
2.4. Power Error
2.4.1.1.1.1 Faulty Relay Power
2.4.1.1.1 Faulty Switching Pre-Regulation
2.4.1.1 Faulty Sensor Power Regulation (VOC5)
2.4.1 Faulty CAN Bus Power
2.4.2.1.1.1 Faulty Relay Power
2.4.2.1.1 Faulty Switching Pre-Regulation
2.4.2.1 Faulty Sensor Power Regulation (VO6)
2.4.2 Faulty Sensor Power
2.4.3.1.1.1 Faulty Relay Power
2.4.3.1.1 Faulty Switching Pre-Regulation
2.4.3.1 Faulty Main CPU Power Regulation (VOM5)
2.4.3.2.1.1 Faulty Relay Power
2.4.3.2.1 Faulty Switching Pre-Regulation
2.4.3.2.2 Faulty Battery Power
2.4.3.2 Faulty Main CPU Power Regulation (VOM2)
2.4.3.3.1 Faulty Battery Power
2.4.3.3 Faulty Main CPU Power Regulation (VOS2)
2.4.3 Faulty Main CPU Power
2.4.4.1. Faulty Sub-CPU Power Regulation (VOM5)
2.4.4.1.1.1 Faulty Relay Power
2.4.4.1.1 Faulty Switching Pe-Regulation
2.4.4.2 Faulty Sub-CPU Power Regulation (V0S5)
2.4.4 Faulty Sub-CPU Power

Figure 6.6-1. Fishbone Diagram of Postulated UA Causes

While not absolute, in general, the NESC team focused on those failures that could increase the throttle opening, and do not set a DTC. Any failure or set of failures that were identified as a potential source of a UA, without generating a DTC, is discussed in the body of the report in their functional area. Those elements that have been identified as potential sources of UAs are identified by a red square in the diagram and are summarized in Table 6.6-1. This is a subset of all possible failures and does not include design features that intentionally open the throttle or all possible variations of a given failure mode.

Table 6.6-1. Fishbone Summary of Potential UA Sources

Major Fishbone Area	Failure Mode Category	Finding	Addressed in Report Section
1 Throttle Control	Postulated Throttle Position Sensors Supply (Vc) Increased Resistance	F8	6.6.1.2.1
	Postulated Throttle Position Sensors Return (E2) Increased Resistance with Learning	F8	6.6.1.2.2
	Throttle Postulated Resistive Fault Summary	F8	6.6.1.2.3, 6.9
	Throttle Stuck	F8	Appendix B-1
	Throttle Motor Drive electronics PWM, H-Bridge, transistor failure, and or latch up	F8	Appendix B-1, Appendix-C, 6.9
	Single event upset	F8	Appendix B-1
	EMI	F9	Appendix B-1, 6.8, 6.9
2 Pedal Command	Postulated Pedal Position Sensors Supply (Vc) Increased Resistance with Learning		6.6.2.2.1
	Pedal Single Faults of VPA1 or VPA2	F6	Appendix B-2
	Pedal Postulated Dual Faults placing VPA1 and VPA2 in the operational lane	F6	6.6.2.2.2, 6.9
	Hall Sensor External Magnetic Fields		6.9
	Signal Aliasing of VPA1 and VPA2:		6.6.2.2.3, 6.8
	EMI, Noise Coupled into VPA1 and VPA2	F9	Appendix B-2, 6.8
3 Idle Speed Control	Engine Coolant Temperature	F8	6.6.3.1, 6.8
	Engine Speed signals		6.6.3.4, 6.8
	Compensate for Additional Engine Loads		6.6.3.5
4 Cruise Control	Cruise Control Signal	F7	6.6.4.4
	Cruise Control Brake Switch Cancel		6.6.4.3
	Cruise Control Gear Shift Cancel		6.6.4.5
	Vehicle Speed Sensor Failure		Appendix B-4
5 Transmission Shifting	Sensing incorrect gear selection	F9	6.6.5, Appendix B-5
6 VSC	Sensing incorrect vehicle motion	F9	6.6.6
7 Power	+12v or +5v Ripple or Transients		6.6.7, 6.8, Appendix B-6
8 Software	Coding Defects	F10	6.7, Appendix B-7
	Algorithmic Flaws		
	Task Interference		
	Insufficient Fault Protection		
9 Environmental	EMI Radiated Fields	F9	Appendix B-8, 6.8, 6.9
	EMI Conducted Noise	F9	
	EMI Transients		
	Single Event Upset		Appendix B-8, 6.9
	Electrostatic Discharge		
	Mechanical Vibration		
	Thermal		

To decompose this system, the design was separated into the major control loops or functional areas in the ETCS-i that regulate engine power output: throttle control, pedal control, ISC, cruise control, transmission control, and VSC. The main focus of this study was in the first three control loops. Cruise control was considered a potential cause of UA because the electronics is placed in direct control of the vehicle speed. There were a number of VOQs involving cruise control. However, most of these could be traced to normal operational characteristics of the cruise control function. The maturity of cruise control systems and the multiple driver mitigations and electronic control limitations made this functional area a less likely candidate for causing UAs than the other throttle control electronic functional areas.

The remaining two control loops, transmission control and VSC were studied briefly to determine the magnitude of their influence on throttle opening. They were determined to have limited ability to influence throttle opening.

The following sections will cover the functional control areas starting with the inner most control loop (i.e., the throttle control). Although not a direct link to controlling the throttle, the power supply system effect on throttle opening was also evaluated and is presented at the end of the functional areas. The last three areas shown in the fishbone diagram include software error, environmental effects (e.g., mainly EMI), and mechanical effects (e.g., throttle binding). Software is addressed in Section 6.7, EMC/EMI, and mechanical effects in Section 6.8. Several external theories were also studied by the NESC team, and these are dispositioned in Section 6.9.

It is important to recognize that the vehicle has nominal design features which will result in an increased engine speed and these are not considered faults. Some examples of nominal design features are:

- The vehicle is designed to increase the engine speed under the increased load of the air conditioning.
- The transmission torque converter lock-up is another design feature which results in an increased engine speed. See Section 6.6.5, Transmission Control.
- Under cold conditions, the vehicle is designed to idle faster and to gradually decrease the idle as the engine warms.
- The engine fuel injection and ignition timing was delayed as part of the knock sensor software. When the accelerator pedal is pressed the increased airflow combines with the fuel resulting in a driver-sensed delayed acceleration greater than when this condition is not present.
- When the cruise control is in use on hilly terrains, the automatic transmission may downshift to maintain set speed which results in significantly higher engine speeds that some consumers may interpret as an aggressive vehicle response.

6.6.1 Throttle Position Control Functional Area

6.6.1.1 Detailed Implementation Description

The throttle control loop maintains the throttle motor at the commanded throttle position based on throttle position sensor feedback. The throttle functional block diagram that describes this operation is shown in Figure 6.6.1.1-1. The control loop consists of six major components: 1) the throttle motor and its associated mechanisms, 2) the motor drive IC, 3) two throttle position Sensors, 4) the Sub-CPU, 5) the Main CPU, and 6) the software for both the Main and Sub-CPUs. Refer to Figure 6.7-1 for the Software Block Diagram.

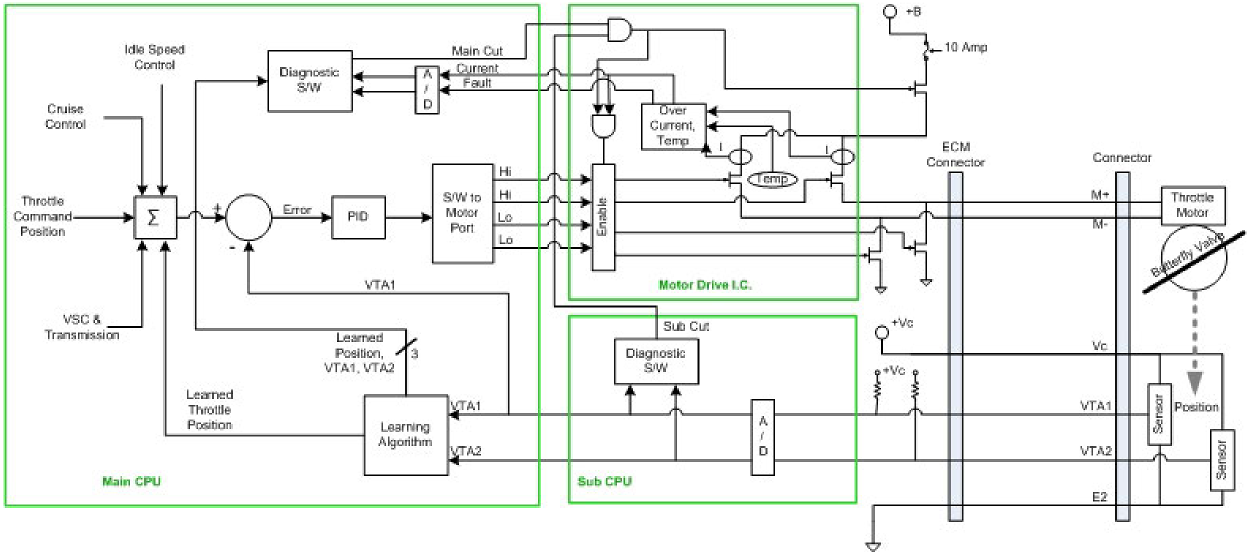


Figure 6.6.1.1-1. Throttle Valve Control Block Diagram

Once the Main CPU determines the desired throttle drive position, it outputs the commands to the H-Bridge on four signal lines (HI, HI, LO and LO).   The circuit path from these four lines to the actual motor winding is an important electrical area to review since it is beyond the direct CPU control yet faults exist which can drive the throttle valve motor. Faults in this area are captured by either over current and/or over temperature sensing. The throttle valve motor is a DC motor that operates on PWM drive to control the current delivered to the throttle motor and thus control the throttle valve position. The PWM signals are supplied thru the M+ and M-lines which can supply pulses of either polarity to the motor by an “H-Bridge” circuit. The throttle valve is counteracted by a spring, and upon removal of power to the throttle motor, the throttle valve will return to its “spring detent” position (6.5 degrees above fully closed position).

Power to the throttle motor is controlled by the Main CPU via the Motor Drive IC and three external FET switches. One external FET switch is in series with fused +12V drive power to the IC and can be switched on or off by either the Main or Sub-CPU (as notionally represented as "sub cut" and "main cut" in the block diagram). In actuality these are complementary logic signals. The other two external FETs are a part of an H-Bridge that switches either side of the motor winding to ground in response to PWM signals (two HI and two LO) from the Main CPU at approximately 500 Hz. The other two H-Bridge FETs PWM switch the +12V power and these are located inside the IC. These internal FETs also have a current monitoring feature, which provides an analog current signal to the Main CPU. If the measured current exceeds threshold values a limit flag is sent to the Main CPU and can cut off PWM drive signals to the H-Bridge. The IC also has a signal from the Sub-CPU and a different signal from the Main CPU that can inhibit PWM drive signals to the H-Bridge, as shown as inputs to the Motor Drive I.C. in Figure 6.6.1.1-1. Also, certain sensed voltage conditions can trigger an IC reset with PWM drive signal inhibit, and an internal IC temperature sensor that can inhibit the PWM signals.

The throttle position sensors are used by the ETCS-i to monitor and verify the physical angle of the throttle valve. These consist of two sensors, operated in parallel, sharing the same power supply and return lines. Two basic types of throttle position sensors have been used by TMC since the inception of the ETCS-i, resistive sensors for MYs 2002 and 2003, and Hall Effect sensors for all Camry models from MY 2004 and beyond. The potentiometer sensor uses a mechanical contact and thus would be more prone to wear out failure modes than the non-contact Hall Effect sensor. It is important to point out that a poor electrical connection in the potentiometer contacts would lead to an open circuit which combined with the internal ECM pull up resistor would result in generation of a DTC and entry into a fail-safe mode of operation. These sensors monitor the physical angle of the throttle valve via a mechanical or magnetic coupling between the sensors and the valve, for the resistive sensor or Hall Effect sensors, respectively. Figure 6.6.1.1-2 shows the throttle sensor output voltage relation between VTA2 and VTA1 for a MY 2007 Camry. This relationship is the same for all sensor types.

To effectively understand and evaluate the range/area of valid or invalid values, the NESC team used the software models and vehicle hardware to generate "diagnostic maps" notionally shown in Figure 6.6.1.1-2. These maps, or plots, identify the relationship between the two VTA1 and VTA2 throttle position sensor voltages, with VTA1 as the horizontal axis and VTA2 as the vertical axis. The acceptable range of throttle sensor values creates an operational "lane" on these maps where the sensor voltages can reside without generating a DTC. Other throttle sensor value relationships outside this operational lane can generate DTCs and possible fail-safe modes.

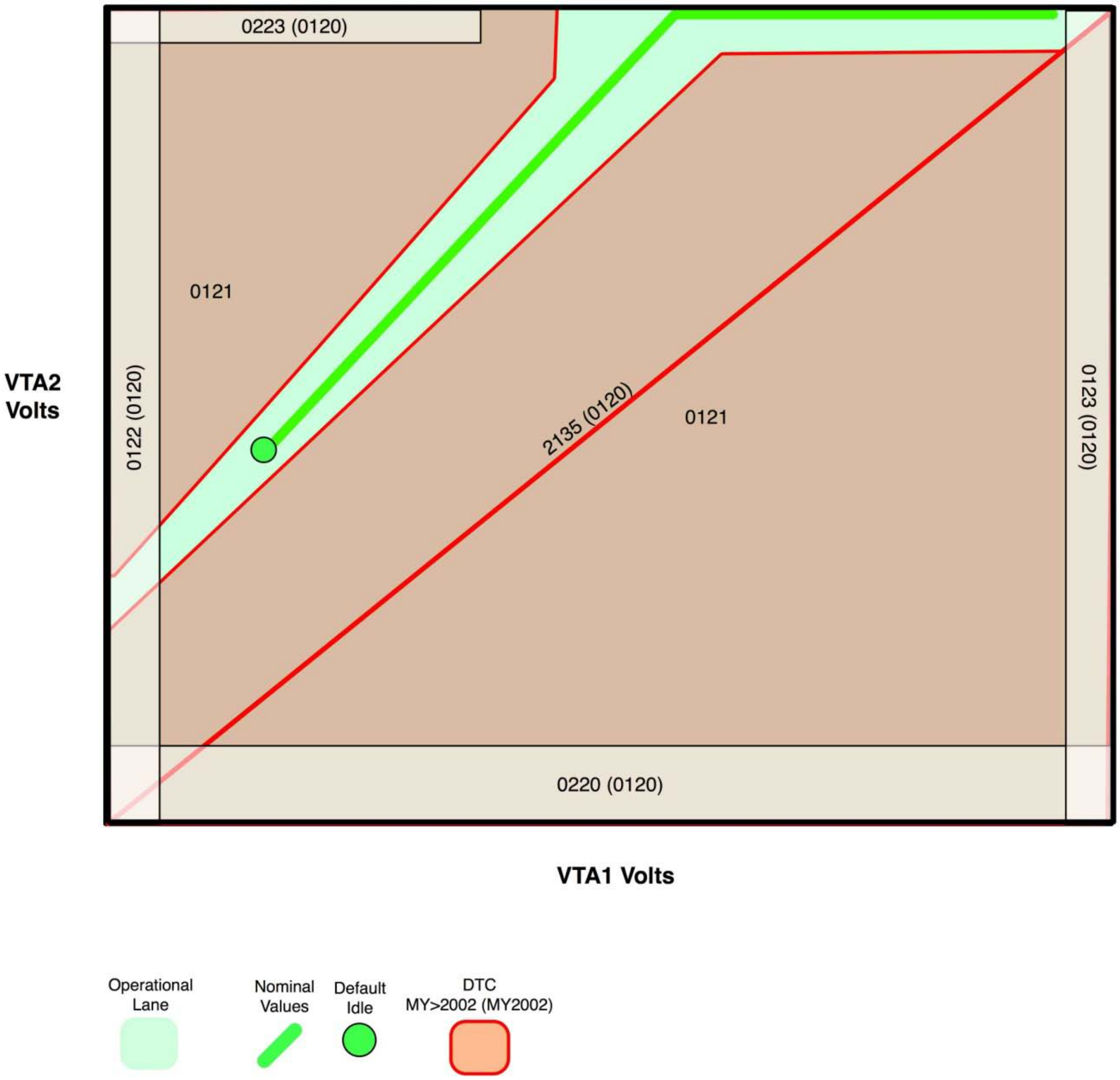


Figure 6.6.1.1-2. Notional ThrottleValve Sensor Output Voltage Relation between VTA2 and VTA1 and the DTCs

The monitor or Sub-CPU reads and converts the accelerator pedal sensor signals, the cruise control command, and other auxiliary sensor signals. This information is then transmitted by DMA interface to the Main CPU for respective processing.

The Main CPU calculates the desired throttle valve angle by using a Proportional, Integral, and Derivative (PID) control algorithm with the information from the pedal position sensors, the ISC, the learned spring detent value, the auxiliary sensors and the cruise control set value. Figure 6.6.1.1-3 shows the contribution to the commanded angle from all associated sensors. The calculated angle is then converted into desired duty cycle. This duty cycle is then sent to the Motor Drive IC to control the throttle valve angle.

The H-Bridge circuit is controlled by the ETCS-i software in the form of four signals (HI, HI, LO, and LO). These four signals open or close as appropriate the two internal high side FET switches of the H-Bridge drive IC and the two external low side FET switches of the H-Bridge drive circuit. The 4 signals are based on conversion from a calculated duty cycle command coming from the PID control software. The duty cycle dictates the closing/opening rate which is controlled by changing the on and off times of four FETs. As previously noted, the H-Bridge drive IC is thermally protected and current limit protected and cuts off the motor drive if an over temperature or over current condition occurs.

The main function of the PID controller is to assure the throttle value is properly positioned per the desired throttle command. If the throttle valve is not in its desired position, then the PID receives an error signal driving the throttle motor and valve towards the desired position. If the motor does not respond and an error signal persists, the integral term of the PID controller will integrate the error resulting in more motor torque until the electronics current limit is reached setting a Stuck Open or Stuck closed DTC.

The PID controller involves three separate parameters: the proportional, the integral and derivative values, denoted P, I, and D. The proportional value determines the reaction to the current error, the integral value determines the reaction based on the sum of recent errors, and the derivative value determines the reaction based on the rate at which the error has been changing.

The input throttle command, which the PID controls to, is a combination of the throttle request from the pedal/cruise/VSC, the request from the ISC, and the learned throttle spring position.

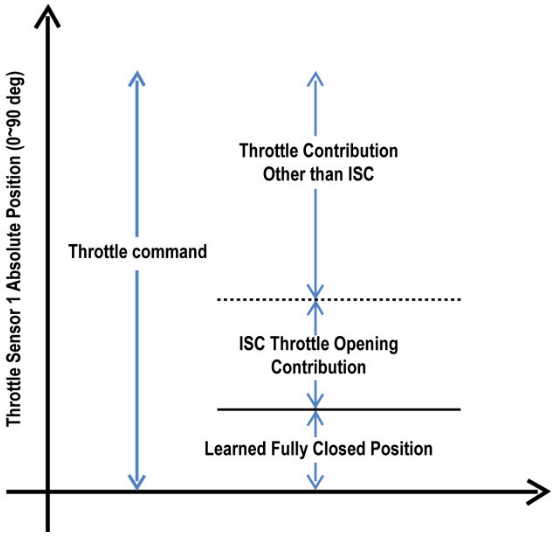


Figure 6.6.1.1-3. Contributions to Throttle Command

The base for the throttle command comes from the learned fully closed value. This value represents the position of the throttle valve when it is not actively controlled. This value is "learned" from [redacted] ms after ignition turn-on, when power is not applied to the throttle motor and it is assumed to be held open by the spring only at its "spring detent" position (6.5 degrees above fully closed position). This value is stored for future ignition key cycles. During the [redacted] ms learning period, if a sensed position difference between the previous and current ignition key cycle (trip) is greater than [redacted] degree, the new learning value is adjusted by a maximum of [redacted] degree per ignition cycle.

The learned value is the foundation for the determination of all other throttle control, including diagnostics. The learned throttle value is used in the determination of thresholds. Note that if the throttle diagnostics determines the existence of a fault, the learning is not reset until ignition off.

6.6.1.2 Throttle Control Loop Sensitivities and Postulated Faults

Figure 6.6.1.2-1 shows the summary of postulated faults that might possibly produce a UA identified from the fishbone diagram analysis for the throttle control functional area. Based on the preceding understanding of the throttle control design, a fishbone diagram was generated and used to identify potential sensitive entry points into the throttle control loop. See Appendix B for the entire fishbone analysis results. In the throttle control loop two sensitivities were identified where postulated faults can produce an increase in engine speed. The fishbone identified a poor electrical connection either in the throttle position sensor and wiring, ECM circuit card, and/or ASIC hardware may combine with the learning algorithm to create the two potential faults listed below. In addition, the fishbone identified sensitivity to coupled energy, which is discussed in Section 6.6.1.2.3.

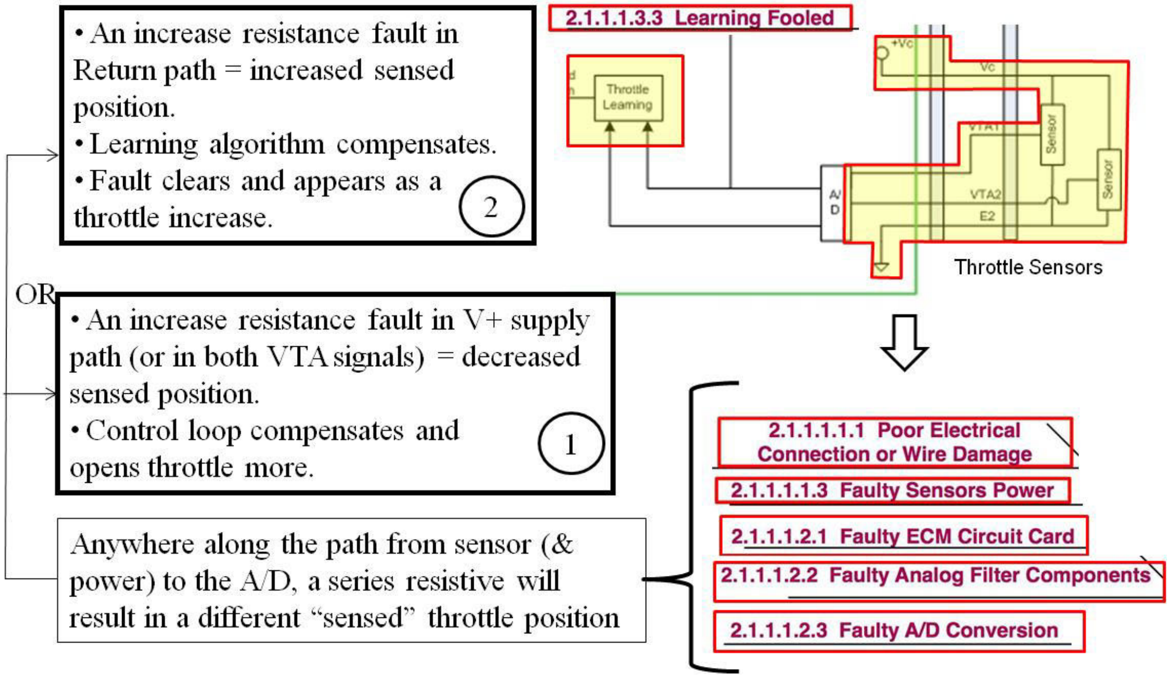

• An increase resistance fault in Return path = increased sensed position.
• Learning algorithm compensates.
• Fault clears and appears as a throttle increase.
2
OR
• An increase resistance fault in V+ supply path (or in both VTA signals) = decreased sensed position.
• Control loop compensates and opens throttle more.
1
Anywhere along the path from sensor (& power) to the A/D, a series resistive will result in a different "sensed" throttle position
2.1.1.1.3.3 Learning Fooled
Throttle Learning
+Vc
Vc
VTA1
VTA2
E2
A/D
Sensor
Sensor
Throttle Sensors
2.1.1.1.1.1 Poor Electrical Connection or Wire Damage
2.1.1.1.1.3 Faulty Sensors Power
2.1.1.1.2.1 Faulty ECM Circuit Card
2.1.1.1.2.2 Faulty Analog Filter Components
2.1.1.1.2.3 Faulty A/D Conversion

Figure 6.6.1.2-1. Summary of Postulated Faults Identified by Throttle Function Fishbone Diagram

6.6.1.2.1 Postulated Throttle Position Sensors Supply (Vc) Increased Resistance

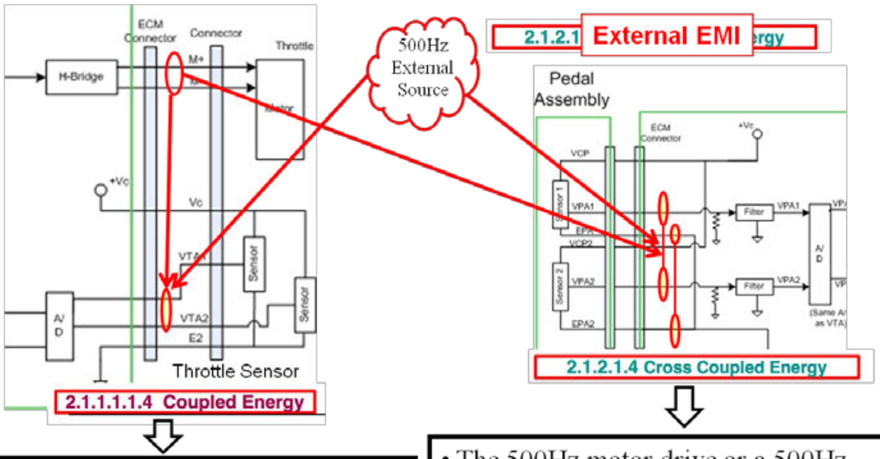
A postulated resistance (<40Ω) increase on the throttle sensor voltage supply (Vc) wire/connectors will lower the voltage at the sensors and correspondingly the VTA signals for the position sensors. The control loop will respond by opening the throttle to compensate for the drop in voltage. The functional effect of dropping the supply voltage applies to both the Hall Effect sensors and the potentiometers. The postulated fault will result in a throttle opening of approximately 3 degrees, with no generated DTC. If large resistance is used, then the system may generate a DTC, taking appropriate action (limp home mode). A vehicle throttle Vc resistance test was performed on the MY 2005 L4 Camry by adding a serial resistance in the throttle Vc supply line. A resistance of approximately 30 to 40 ohms resulted in a throttle position increase of 3 degrees in neutral, increasing the resistance resulted in DTC P0121. However the vehicle engine speed will be limited by the fuel cut design feature as explained in Section 6.4.

6.6.1.2.2 Postulated Throttle Position Sensors Return (E2) Increased Resistance with Learning

A postulated resistance (<25Ω) increase on the throttle sensor supply return (E2) wire/connectors will increase the sensors signal levels resulting in a lower engine speed. The learning algorithm will compensate and learn this new sensor value. If the fault is removed, the sensor voltage will drop and the control loop will compensate by opening the throttle. This effect applies to both the Hall Effect sensors and the potentiometers. By design the learning algorithm software limits the adjustment of the learned fully-closed position to [redacted] degree per ignition cycle. Testing indicated a resistance up to 25 ohms in the return line will drop the engine speed as explained above; fault resistances of higher values resulted in a DTC being generated. If the fault is removed, then the engine speed will increase by approximately 200 to 500 rpm (in neutral) or [redacted] degree as indicated by the software analysis.

6.6.1.2.3 Signal Aliasing of VPA1 and VPA2

Figure 6.6.1.2-2 indicates the postulated EMI faults as identified from the fishbone analysis. Three different tests uncovered a 500 Hz sensitivity; the noise injection common to both VPA signals, noise injection on VTA1 signal, and the vehicle level conductive EMC testing.



- The 500Hz motor drive or a 500Hz external source corrupts VTA1 signal resulting in lower "sensed" throttle opening and the control loop compensates by opening throttle.

- The 500Hz motor drive or a 500Hz external source corrupts **both** sensor signals or signals' return resulting in higher "sensed" pedal position and control loop responds by opening throttle.

Figure 6.6.1.2-2. Summary of Postulated EMI Faults Identified from Fishbone Analysis

On a simulator, a signal was injected in both VPA signals between their return lines (EPA1 & EPA2) and the ECM common ground. The results indicated a decreasing system response as the frequency was increased. However, as the (0.4Vpp) noise source on VPA signal return was increased to a frequency of 500 Hz, a 2 Hz signal (beat frequency with the internal 500Hz A/D sampling) of 0.2Vpp was observed on VTA as shown in Figure 6.6.1.2-3. Note the results shown are for a simulator without air flowing through the throttle body and are intended to describe the electrical response and not intended to describe an actual vehicle response.

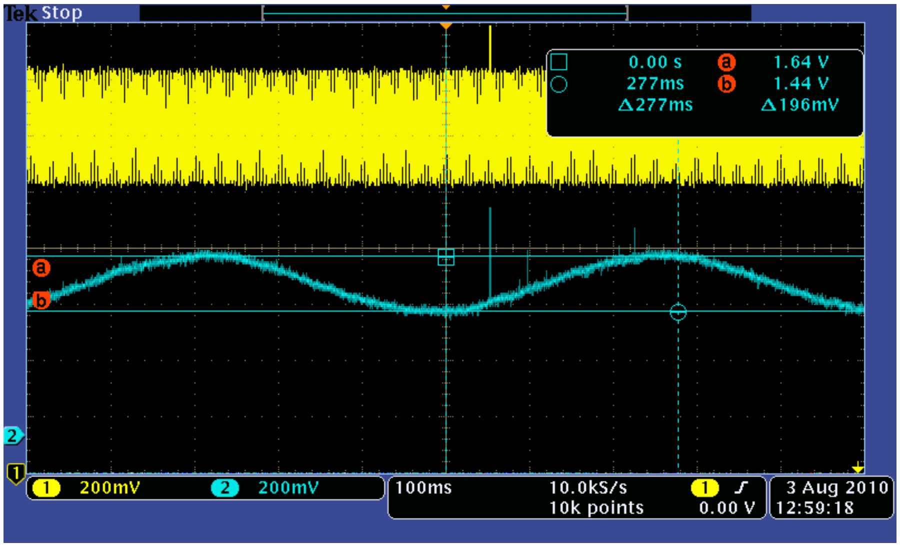


Figure 6.6.1.2-3. 500Hz injected common to both VPA signals (top Yellow trace) results in driving the motor and roughly 2 Hz aliasing sensed on VTA (bottom Blue trace)

A test of injecting noise in series with the VTA1 signal resulted in a similar frequency response of 2 Hz. The different beat frequency was expected since the beat frequency is the difference of the A/D convertor sampling frequency and the injected frequency.

Spice modeling indicated the analog filter attenuation at 500Hz was -11dB, although the exact required level is not known for this system, this level of attenuation may not be sufficient to serve as an anti aliasing filter.

Additionally, the vehicle-level EMC testing injected audio noise (at 2Vpp) on both VPA signals at 500 Hz resulting in a vehicle engine response of 5000 rpm in neutral. The increased engine speed was observed from 400 Hz out to the kilohertz range with a peak speed at 500 Hz. The higher frequency sensitivity suggests rectification of the injected noise and is not directly related to the 500 Hz sensitivity. The vehicle level testing indicated that the throttle increase was directly proportional to applied noise level and the influence was not a latching effect. That is, if the noise was removed the effect was removed. Recall from the earlier section that for full throttle, VPA1 must be $\geq$ 3V, but cannot exceed 4.8V.

Field reports were examined for signs of noise coupling into the throttle sensors. There were two Field Technical Reports (TQCN/TOY-RQ-00074023_FTR-7QR101241 and TQCN/TOY-RQ-00074046_FTR-7QK101441A) that mention surging with a cold engine. The reports suspect a splice in the throttle sensor return wiring as the problem. The surging was eliminated by restoring the ground connection. Field report TQCN/TOY-RQ-00074514 describes a noise source coupling into the VTA signal resulting in “Surging approximately 100 rpm every 3-5 seconds”. The field report’s oscilloscope shows the VTA1 with a narrow ~2V positive pulse immediately followed by a negative 0.8V pulse in the 1 millisecond range, (no repeat rate was cited in the report). The surging was eliminated by replacing the harness. According to these field reports, noise coupling into VTA1 did not create a constant throttle command.

When an external excitation around 500 Hz was applied to the VPA signals, an opening of throttle was observed consistent with a beat frequency with the 500Hz A/D sampling. However, no internal 500 Hz source was identified in the design or observed in EMI testing with sufficient amplitude to create throttle openings.

6.6.1.2.4 Throttle Postulated Resistive Fault Summary

Testing demonstrated that both postulated resistive faults mentioned above open the throttle, but are limited to less than 5 degrees opening. The postulated high resistance in the power line is self limiting by the fact that the compensated throttle position cannot be larger than the supply voltage would allow. The time duration of an engine speed increase would be a function of the presence (or the lack of it depending on the fault type) of the fault in the power line. As long as the power line fault was present, the increased speed would occur. The postulated fault in the return line requires learning therefore the duration will be a function of the learning. Key cycles will result in a new learned value for the throttle valve fully-closed learned value. As mentioned in Section 6.4, the fuel cut feature also can limit these postulated faults if the engine speed reaches 2500 rpm.

6.6.2 Accelerator Pedal Control Functional Area

6.6.2.1 Detailed Implementation Description

The accelerator Pedal Functional area uses the pedal position as the main control input with the driver closing the loop. In this control loop the pedal position is read from the two pedal sensors and these position readings provide to the ETCS-i the primary driver demands for acceleration. This demanded acceleration is based upon the difference between the accelerator pedal null position at rest, and the driver’s pedal pressed position.

The two pedal sensor values are verified for acceptance against a range of values. Sensor values outside an acceptable range are detected to produce fail-safe behaviors. Both the pedal null sensor values and the range of acceptable values are dynamic. During nominal operation, the pedal null value is learned, and the acceptable range of values shifts to accommodate the ETCS-i operations.

When a driver’s foot is sensed as being off the accelerator pedal, the pedal returns to the released position, and the pedal sensors report this null position to the ETCS-i. The ETCS-i software contains a pedal learning algorithm that compensates for variations in this absolute sensor null position. At times when the pedal is released, during startup, nominal driving, and while in cruise control, the pedal learning can execute and determine a new null position.

The accelerator pedal system also contains software logic that expands acceptable operational ranges during operation after encountering off-nominal pedal sensor inputs or power on CPU reset. This permits the allowed values of the pedal sensors to change during vehicle operation, and alters the values that generate DTCs or determine fail-safe conditions.

The pedal functional area is shown in Figure 6.6.2.1-2. For pedal position feedback, each position sensor has dedicated power and return lines. From 2002 to 2006, the sensors were potentiometers and in 2007 the sensors changed to Hall Effect sensors. For Camry, the Hall Effect sensors used are manufactured by either Denso or CTS. The two VPA signals enter the Monitor or Sub-CPU and are converted from analog to digital, and then they are passed to the Main CPU software.

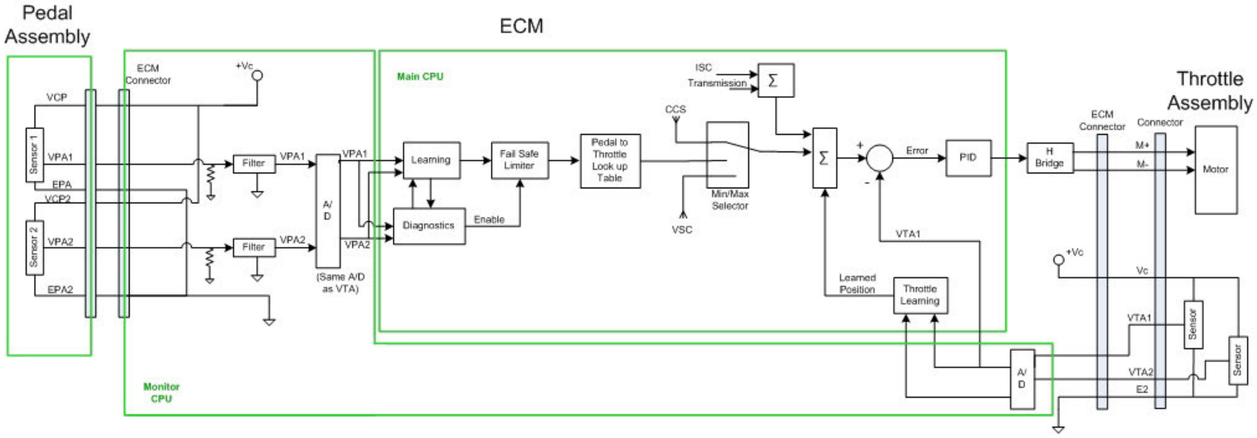


Figure 6.6.2.1-2. Block Diagram of Pedal Control Function

The software controls the throttle valve position by measuring the pedal command angle and comparing it to the learned pedal released value. Using the command and the learned pedal release value, pedal diagnostics are performed. When a fail-safe flag is sent from the pedal diagnostic algorithms, certain fail-safe responses are executed to limit the throttle valve opening (limp home mode). The pedal command angle, after going through the diagnostic and fail-safe processing, is converted to a throttle valve commanded angle. The throttle valve command angle from the pedal input is compared to the throttle request from the cruise control system. The greater value of pedal throttle command and cruise control request is then sent to the PID controller as described in the previous section.

The pedal control's primary input comes from two pedal sensors, whose output voltages are VPA1 and VPA2. "VPA1" is used in this document instead of just "VPA" to avoid confusion when referring to the VPA signals as a group. VPA1 is used for primary control and VPA2 is used to check the validity of VPA1. VPA1 and VPA2 can range between 0V and 5V and are offset from each other by 0.8V. The nominal range is shown in Figure 6.6.2.1-3.

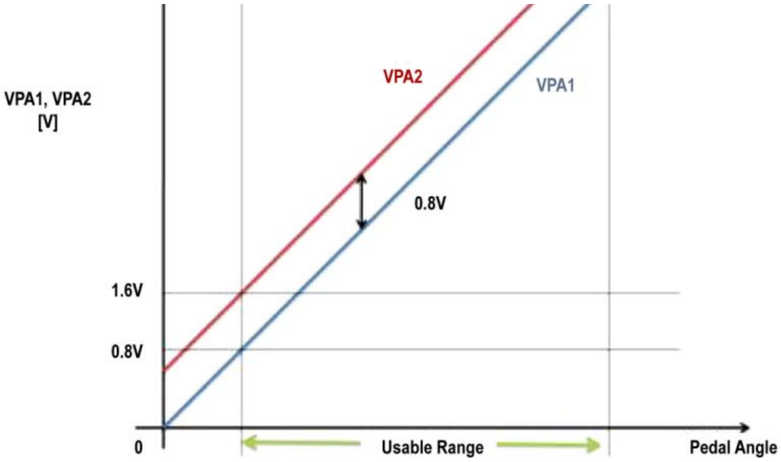


Figure 6.6.2.1-3. Range for VPA1 and VPA2

VPA1 and VPA2 sensors will provide the voltages shown in Figure 6.6.2.1-3. However, the throttle position does not cover this range. The useable range refers to the pedal stroke from not pressed to fully pressed and is not a one-to-one relation to throttle position. When VPA1 is 3.0V or higher, the throttle position remains at wide open throttle (WOT) (i.e., remains at 90 degrees).

The difference between pressed and released pedal positions determines the driver accelerator command. However, the sensed released pedal position is not constant. Due to differences in pedal types and to allow for recalibration during a trip, the pedal input goes through a preprocessing function that recalibrates the pedal sensor input of a released pedal to allow for input variations. The calibration process occurs any time the pedal is determined to be released. The determination of the pedal being released is based on the pedal sensor input values, software state, duration, and timing. The “learned” pedal released value is stored in static RAM (SRAM). The learning value can be reset to the default values if a fail-safe flag is sent from the pedal diagnostics. This reset implements protection against learning values as a result of inputs from faulty sensors. The learned values for pedal released ranges from 10 to 35 degrees (absolute) for VPA1 and [redacted] degrees for VPA2.When the pedal is determined to be pressed, the pedal sensor input is compared to the learned pedal released value and it is this difference that is used as the pedal command.

Based on individual sensor and sensor-to-sensor correlation, checks are performed to determine the validity of the sensor data entering the CPU as described in Appendix A. To effectively understand and evaluate the range/area of valid or invalid values, the team used the software models and vehicle hardware to generate “diagnostic maps” as previously described in the throttle section that identify the relationship between the two VPA1 and VPA2 pedal position sensor voltages. The acceptable range of pedal sensor values creates an operational lane on these maps. Other pedal sensor value relationships outside this operational lane can generate DTCs and possible fail-safe modes.

Expanded thresholds for acceptable pedal values can occur whenever the battery voltage has been removed and restored, during certain pedal learning failures, and when the DTC P2121 has been detected. These expanded thresholds, or DTC wide thresholds, allow a wider range of pedal voltages to be accepted as operational. Nominally, after the foot-off-pedal position has been successfully learned, the operational lane of acceptable sensor values becomes reduced in width. A notional DTC map is shown in Figure 6.6.2.1-4. The wide allowable operating lane for signal voltages is shown in red.

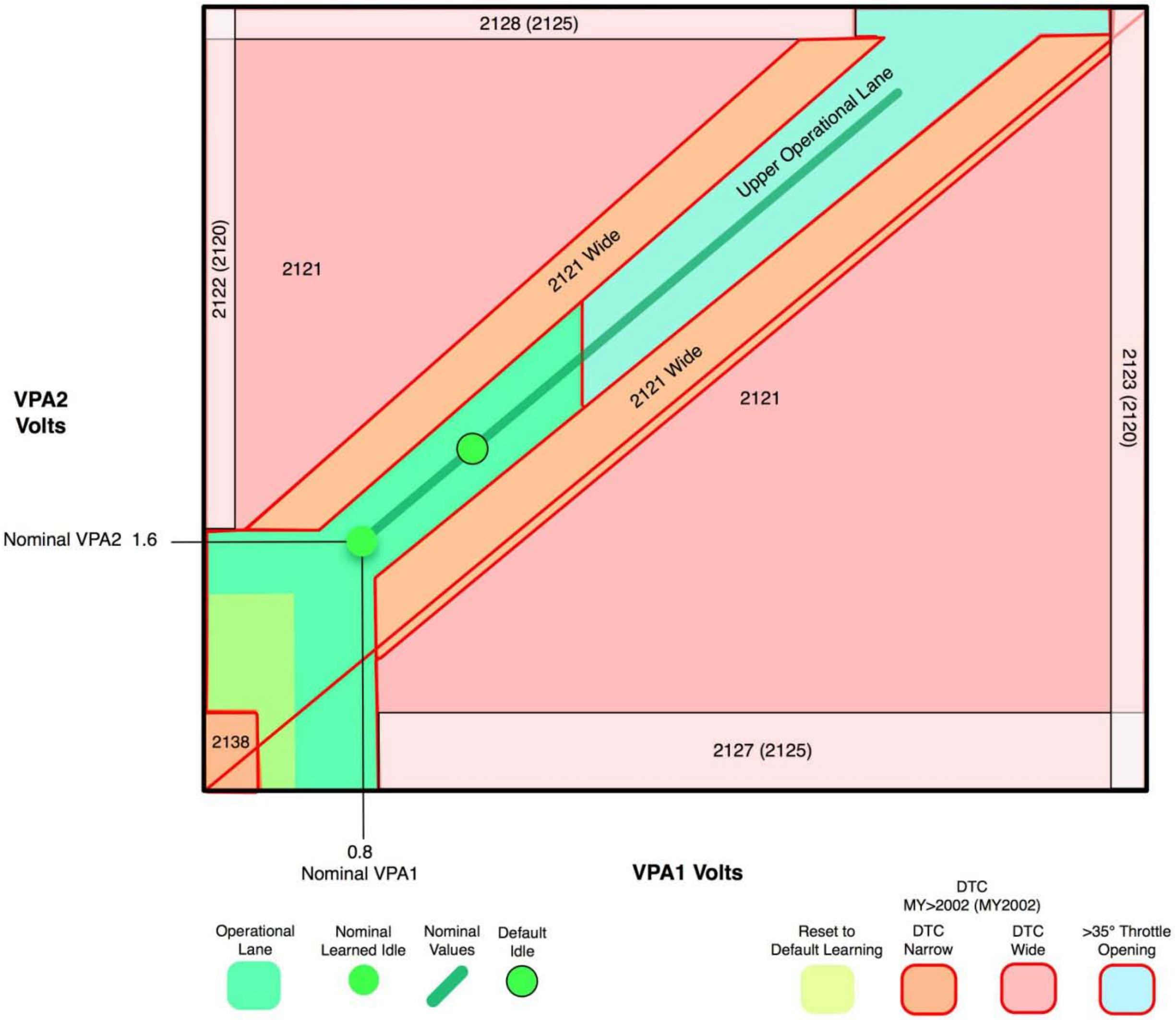


Figure 6.6.2.1-4. Notional Pedal DTC Map, 07 Camry V6, red is P2121 wide limit

The software study focused on the following:

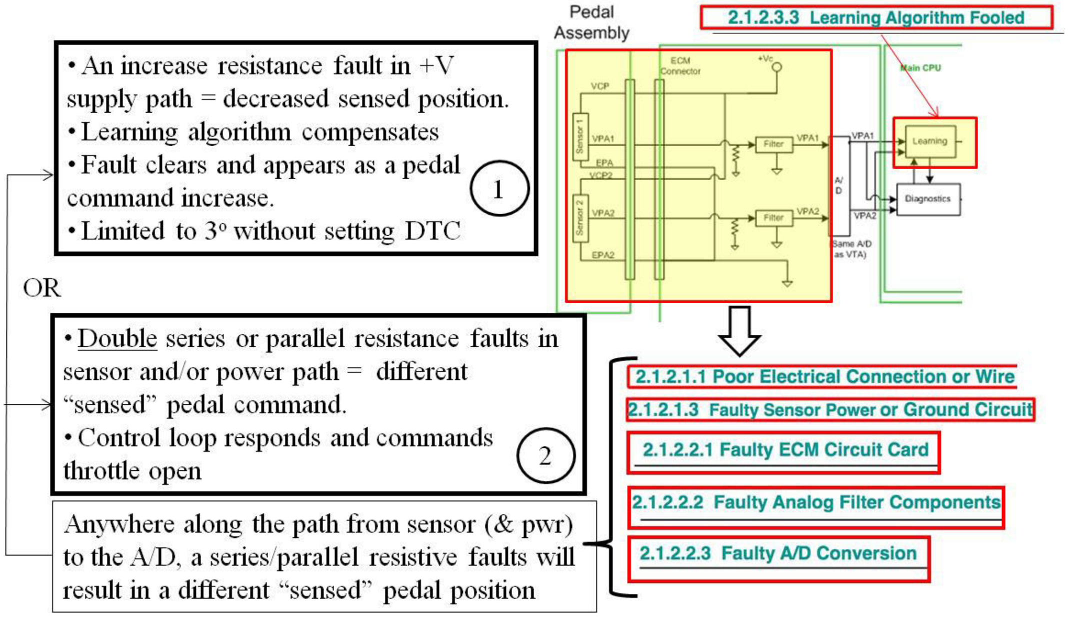
1. Identification of conditions that could allow off-nominal pedal sensor values to be interpreted as a new valid null position. If this were to occur, when the nominal value returns it would be interpreted as a pedal command.
2. Identification of any abnormal conditions that do not produce fail-safe behaviors and do not generate DTCs.

As a result of the software study of pedal learning and these diagnostic maps, focused areas for hardware testing were selected for vehicle tests. The hardware tests of pedal control and results are presented in the following sections.

> ***F-4.*** *For pedal assembly failures to create large unintended throttle openings, failures need to mimic valid accelerator pedal signals.*

6.6.2.2 Pedal Control System Sensitivities and Postulated Faults

The Pedal control system was reviewed for design sensitivities which can result in an unintended increase in engine speed. The pedal function fishbone diagram, provided in Appendix B, was used to identify potential sensitive entry points into the throttle valve control loop and a summary of these faults is shown in Figure 6.6.2.2-1. The fishbone identified that a poor electrical connection anywhere in either the pedal position sensor, wiring, ECM circuit card and/or ASIC hardware may create a potential fault or combine with the learning algorithm previously described to create a potential fault as listed below. In addition, the fishbone identified sensitivity to coupled energy.



- An increase resistance fault in +V supply path = decreased sensed position.
- Learning algorithm compensates
- Fault clears and appears as a pedal command increase.
- Limited to 3° without setting DTC

OR

- Double series or parallel resistance faults in sensor and/or power path = different "sensed" pedal command.
- Control loop responds and commands throttle open

Anywhere along the path from sensor (& pwr) to the A/D, a series/parallel resistive faults will result in a different "sensed" pedal position

1
2
Pedal Assembly
2.1.2.3.3 Learning Algorithm Fooled
ECM Connector
+Vc
Main CPU
VCP
Sensor 1
VPA1
EPA
VCP2
Sensor 2
VPA2
EPA2
Filter
VPA1
Filter
VPA2
A/D
Same A/D as VTA)
VPA1
VPA2
Learning
Diagnostics
2.1.2.1.1 Poor Electrical Connection or Wire
2.1.2.1.3 Faulty Sensor Power or Ground Circuit
2.1.2.2.1 Faulty ECM Circuit Card
2.1.2.2.2 Faulty Analog Filter Components
2.1.2.2.3 Faulty A/D Conversion

Figure 6.6.2.2-1. Summary of postulated faults identified by Pedal Function Fishbone Diagram

6.6.2.2.1 Postulated Pedal Position Sensors Supply (Vc) Increased Resistance with Learning

An increased resistance fault in series with the pedal voltage supply, VCP1 and VCP2, will result in a drop in VPA signals, which will be compensated for by the learning algorithm. Removal of the fault then results in an increase in engine speed. This sensitivity requires postulated faults in two signals and the condition to be learned then removed which the severity is limited to 0.4V in pedal signal or 10 degrees in commanded throttle opening. The fault would be removed by the learning algorithm at the next key cycle.

This postulated failure mode requires both VPA1 and VPA2 to drop in value simultaneously. For example, for VPA1 to learn its lowest false released position just above 0.40V, VPA1 has to drop to just above 0.40V for >0.5 seconds without dropping below 0.40V and, VPA2 has to simultaneously drop below 1.4V, but cannot drop below 1.2V.

When the accelerator pedal is not pressed and the fault is introduced, the accelerator new learned value becomes its lowest possible 9.8 degrees value. If the fault is then removed, the ECM will interpret the step change as a valid pressed pedal and will increase the engine speed. The pedal learning algorithm limits a new value to 0.4V or 10 degrees of commanded throttle opening.

The NESC team demonstrated this postulated double fault by increasing the resistance of up to 1.6 Kohms (for maximum learned values) in both pedal sensor supply voltage (VCP1 and VCP2) signals. Lower postulated resistances in the supply lines had a lower learned value thus lesser effect in engine speed and higher resistances resulted in a DTC for the pedal signal faults. Such specific simultaneous failures affecting both VPA1 and VPA2, to such small voltage ranges (0.4 < VPA1 <0.8 and 1.2 < VPA2 <1.4) are of the same nature as the dual pedal failures described in the upper operational lane, but result in a much smaller throttle opening. Although testing verified that this postulated double fault can result in unintended throttle opening of 10 degrees or less, there were no references found in the VOQ data, field reports or warranty data that confirms this fault is occurring in normal operation. For this fault to occur, corruption of both VCP supply voltages at the pedal would be required similar to the corruption of the VPA signals mentioned below.

6.6.2.2.2 Postulated Faults placing VPA1 and VPA2 in the operational lane

Faults placing VPA1 and VPA2 within their allowable operational lane cannot be detected as a fault, but rather will be interpreted as a valid pedal command and will result in increased engine speed. This sensitivity requires postulated faults in two signals which may result in a pedal command being accepted as valid, and the condition would be present as long as the fault is present.

Figure 6.6.2.1-4 is a plot of VPA1 versus VPA2 and includes the DTC zones. The figure is based on measured data on the MY 2007 simulator and is similar to results obtained on a MY 2005 simulator and point checks on an actual vehicle.

Based on NESC testing and analysis, when the battery is reconnected, for example after maintenance, the DTC limits are set to detect VPA1 and VPA2 voltages within the DTC wide area. Note the operational lane is wider at this time. Upon starting the car, the software tests the VPA1 and VPA2 values. If these values are within the DTC Narrow area, the DTC limits are constrained to the DTC Narrow limits. The DTC narrow limits are maintained for subsequent ignition cycles, and VPA1 and VPA2 values outside this DTC narrow range cause a DTC.

If VPA1 and VPA2 values are detected outside this DTC narrow range, a DTC is generated, and the DTC limits are reset to the DTC wide area. The following analysis used the normal narrow operational lane for calculations of resistance ranges for potential faults.

Since the operational lane area shown in Figure 6.6.2.2-2 is the normal expected operating range of fully functional VPA1 and VPA2 signals, no DTCs or overall system safety checks will catch and mitigate faults in this area. Any postulated fault where the combination of VPA1 and VPA2 signals falls within the operational lane may result in a UA is true for both the Hall Effect sensor pedal and the potentiometer sensor pedal. Faults in the upper operational lane are of most concern since the brake system can be compromised by the loss of vacuum assist if the brakes are pumped at large throttle openings (Section 6.4.2). See Figure 6.6.2.2-2, the blue area represents the operational lane. Within this region the VPA signals are considered valid pedal commands and outside of it they are judged to be invalid VPA signals where a DTC will be generated. The green line represents a nominal VPA signal line where at idle VPA1 = 0.8V and VPA2 = 1.6V. The red line represents the line where VPA1 = VPA2 and note that it is outside the operational lane (but inside the wide lane). A latent resistance fault current path between the

VPA signals if it were to occur can decrease the nominal line in the downward and right direction approaching the VPA1 = VPA2 line. In order to avoid generating a DTC, such a latent resistance must not result in the VPA signals going outside the operational lane. That is, a latent resistance can move the VPA signal from the current line position to the edge of the operational lane. For a Hall Effect sensor and nominal VPA signals (green line), the minimum latent resistance is approximately 200 ohms (to stay in the operational lane if a secondary VPA2 short to +V supply occurs). However, if the VPA signals were closer to the lower operational lane limit, then the minimum latent resistance would be greater, and conversely if the actual VPA signals were closer to the upper operational lane limit, then the minimum latent resistance would be lower.

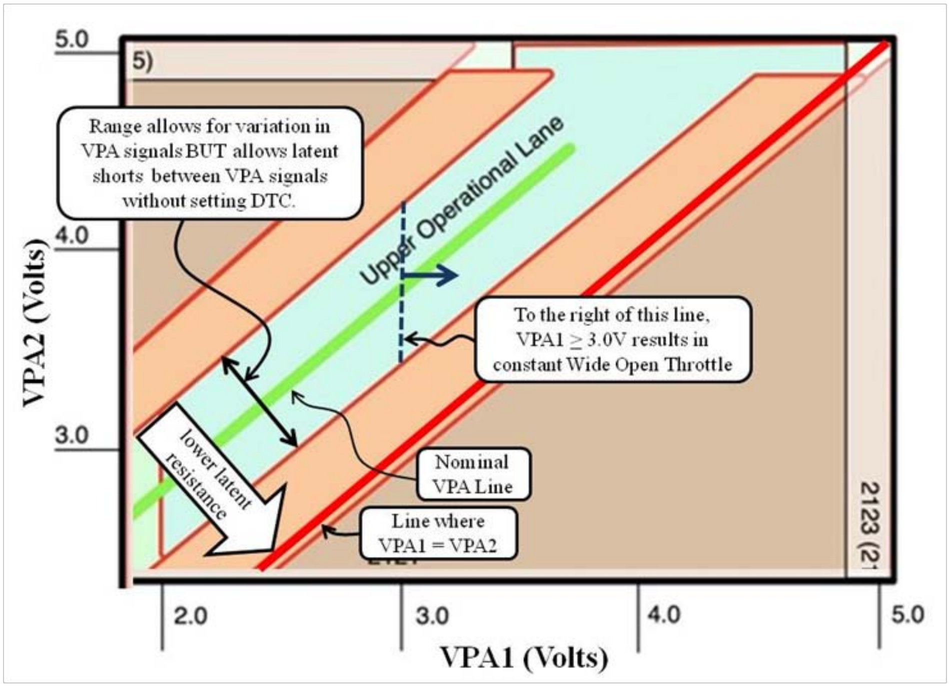


Figure 6.6.2.2-2. The upper operational lane with the latent fault influence and WOT location.

The other key point of Figure 6.6.2.2-2 is the relationship between VPA1 and the throttle position. For nominal VPA signal voltages, VPA1 greater than or equal to 3.0V corresponds to WOT or 90 degree throttle opening. For VPA1 voltages greater than 3.0V, the throttle position maintains a constant WOT. This condition is true only for nominal idle voltages of VPA1 equal 0.8V and VPA2 equals 1.6V. For default learning where VPA1=1.4V, then the WOT VPA1 voltage would be 0.6V higher or VPA1 equal or greater than 3.6V.

Assuming a second anomalous resistive current path fault in the VPA signals to the 5V source Vc, Figure 6.6.2.2-3 shows the chronological steps necessary for a large throttle opening event as described by the VOQ data. Starting on the left, the driver is in control of the vehicle without any indication of a pending problem, then a >25 degrees above idle throttle opening UA occurs due to two anomalous resistive current paths placing VPA1 and VPA2 in the upper operational lane which may last from seconds to minutes followed by the fault clearing allowing driver control again with the fault condition never occurring again in most cases and to not be detected when taken for service in all cases. In VOQ cases analyzed, this type of UA has been reported although in the majority of incidents it was experienced only once. In no known cases (VOQ or otherwise) have the large throttle opening UA conditions been predictably repeated under normally occurring conditions except during NESC tests. Figure 6.6.2.2-3 also includes the possible postulated fault steps in which a UA can occur; either from a latent fault that resides in the design for a period of time then later the second fault condition occurs or also for two faults that occur simultaneously (both within 0.5 seconds time period).

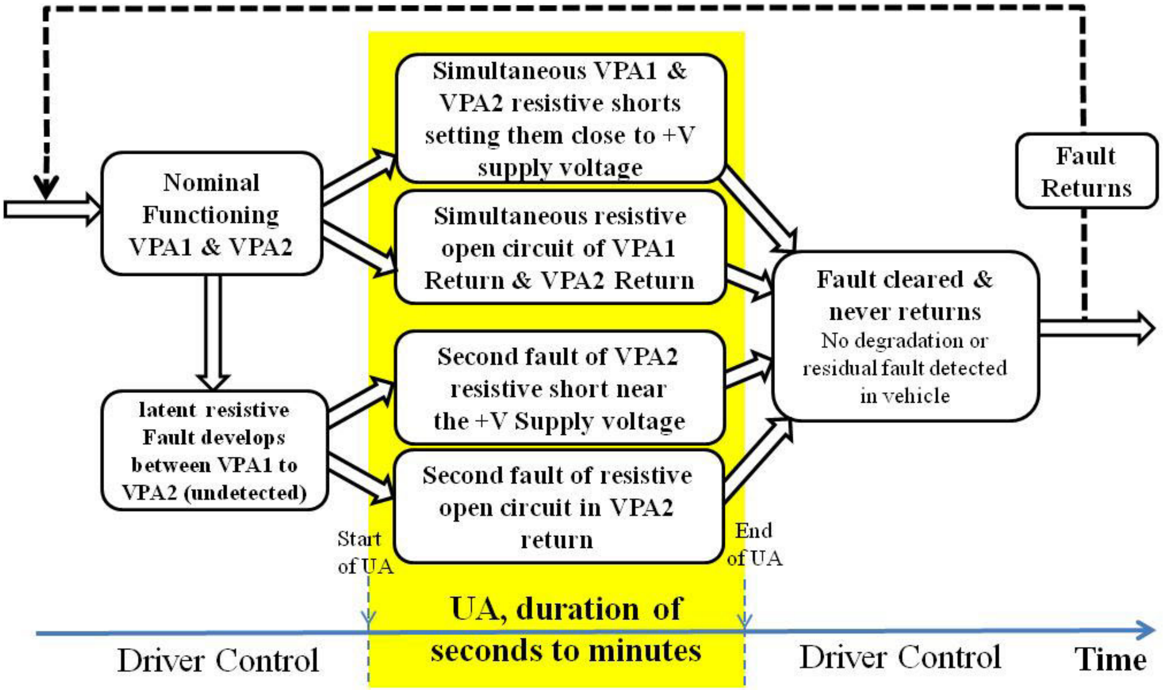

Simultaneous VPA1 & VPA2 resistive shorts setting them close to +V supply voltage
Nominal Functioning VPA1 & VPA2
Simultaneous resistive open circuit of VPA1 Return & VPA2 Return
Fault Returns
Fault cleared & never returns
No degradation or residual fault detected in vehicle
Second fault of VPA2 resistive short near the +V Supply voltage
latent resistive Fault develops between VPA1 to VPA2 (undetected)
Second fault of resistive open circuit in VPA2 return
Start of UA
End of UA
UA, duration of seconds to minutes
Driver Control
Driver Control
Time

Figure 6.6.2.2-3. Chronological steps of a dual fault in the upper operational lane

6.6.2.2.2.1 Latent fault plus second fault

The latent fault plus a secondary fault in VPA2 is of interest because it is the most plausible of the double faults postulated. Latent faults between the two VPA signals allow the two faults to occur at different times and the second fault can be a short to +V supply or an open circuit return.

The latent resistance refers to resistance that can exist between the two VPA signals and go undetected by either the ECM or reading of the diagnostic data through the OBD interface. Potentiometer based sensors, due to their high impedance characteristics are likely to detect the resistances within the ranges that represent a concern however low impedance Hall Effect sensors may not. Figure 6.6.2.2-4 indicates the location of the latent fault in relationship to the VPA signals and the relation of the latent resistance to the resistances for the dual fault to the +V supply.

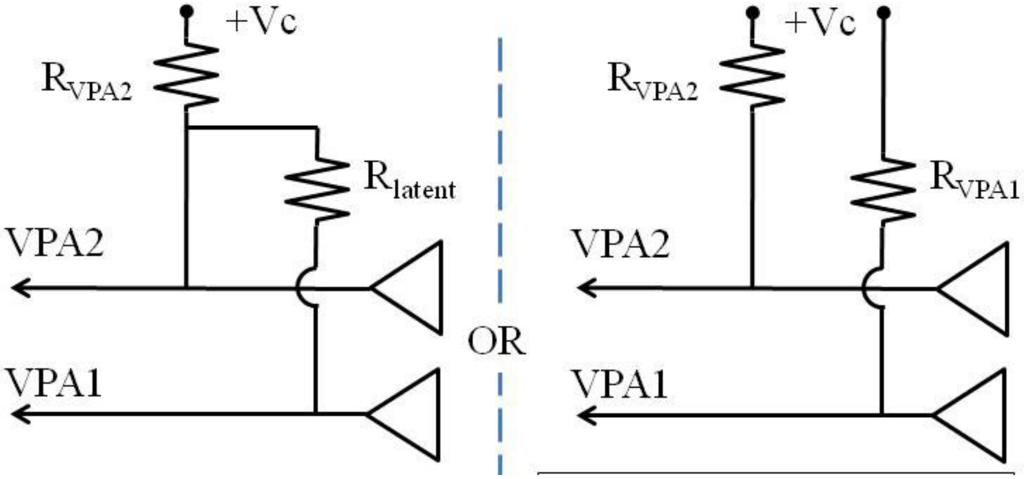


Figure 6.6.2.2-4. Fault resistance locations for the postulated double fault of shorts to the +V supply

A latent fault could exist between the two VPA signals and go undetected (in Hall Effect sensors) within a limited range of resistance values and at some later time the second fault to VPA2 could occur placing the two signals in the upper operational lane. The low output impedance of the Hall Effect sensor amplifier allows the latent resistance to be present yet not impact the circuit performance. As will be shown later, the potentiometer sensor has a much higher output resistance and latent faults of the same resistance (as Hall Effect latent resistance) will result in the signals going outside the operational lane and generating a DTC for most, but not all conditions.

Previous studies on the Hall Effect sensor pedal have shown that 200 ohms latent faults between VPA1 and VPA2 can exist and not generate a DTC.

The potentiometer sensor pedals utilized much higher output impedance limiting the development of external resistance between VPA1 and VPA2 to a minimum of 4.5kΩ resistive faults that typically do not generate a DTC. See Appendix C for additional details.

Figure 6.6.2.2-5 shows the resistance ranges for a latent fault and the second VPA2 fault for both Hall Effect sensor type pedals used in the Camry, those manufactured by Denso and those manufactured by CTS. The vertical lines are the minimum latent resistance for both pedal types that allows the latent fault to go undetected in normal pedal operation. In order to prevent generating a DTC during normal operation, the latent resistance must be greater than 170Ω for the CTS pedal and greater than 130Ω for the Denso pedal. These resistance range plots are similar to Figure 6.6.2.2-6. However, they show the more limited latent resistance ranges.

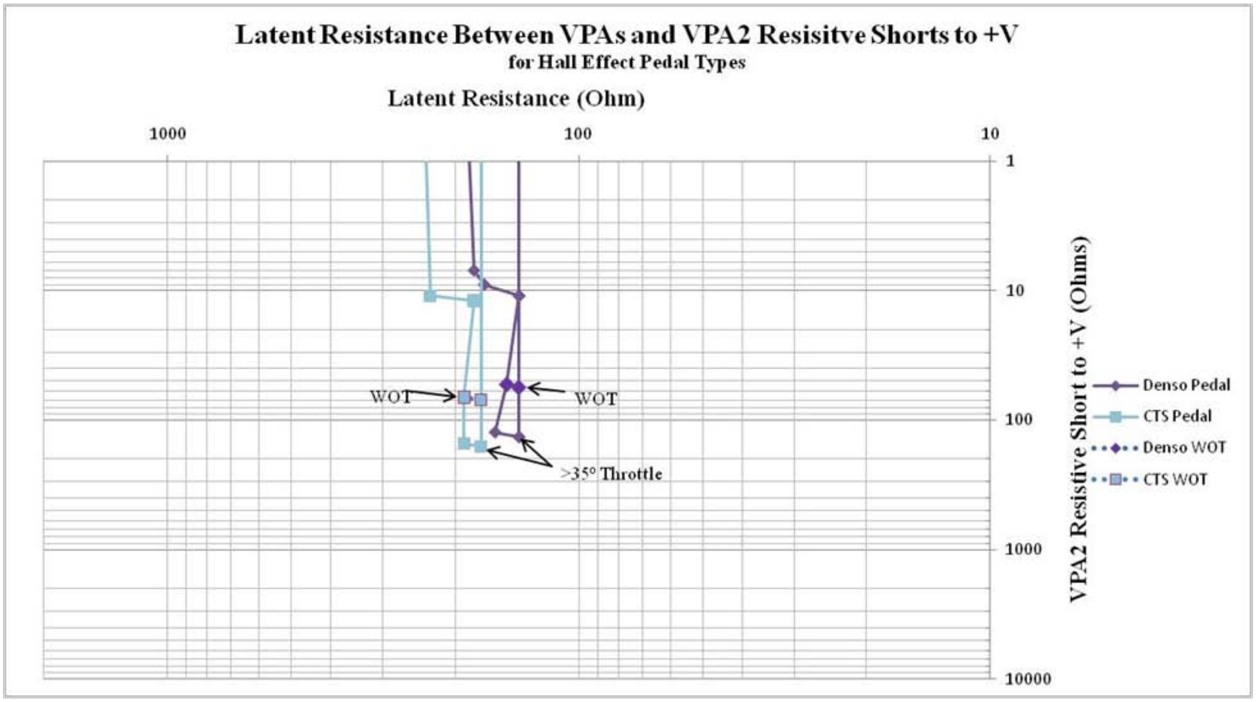


Figure 6.6.2.2-5. For Hall Effect type pedals, resistance range required for latent fault between VPA signals and second fault of VPA2 resistive shorted to +V

The other failure mode identified is a latent fault between the VPA signals with the second fault being a resistive open circuit on the VPA2 return line. The NESC team studied this effect (see Appendix C). For the CTS pedal tested, there was not a resistance range, but rather a single resistance of approximately 170Ω between the VPA signals which placed them in the upper operational lane with a VPA2 return line open circuit of 8kΩ or greater (and not generate a DTC). Since the fault was at the edge of the operational lane, due to natural variances other CTS pedals may have a narrow resistance range allowing this fault to occur and not generate a DTC for the full range of pedal stroke.

For the latent fault plus open circuit of VPA2 return postulated failure mode in the Denso pedal, the latent resistance must be greater than 130Ω, but less than 160Ω and VPA2 return open circuit must be greater than 800Ω to prevent generating a DTC during normal operation (see Appendix C).

6.6.2.2.2.2 Simultaneous Faults

A fault to place the VPA signals within the operational lane can be postulated with either pedal type. However, it requires two simultaneous (within < 0.5 second time period, so as not to set a DTC) resistive faults that must remove themselves (within the same 0.5 second period) after the

UA event. The simultaneous condition is necessary because either fault occurring alone will result in generating a DTC. There are four postulated fault conditions that can place the VPA signals in the upper operational lane, either two simultaneous resistive shorts to the +V supply or two simultaneous resistive open circuits of the supply return or a combination of each fault condition, (one resistive short of a VPA signal to the +V supply and one resistive open circuit on the other VPA signal).

The term “resistive short” is used to signify the resistive condition of a partial or non-zero ohm short circuit. The resistive short for VPA1 must be different than the resistive short of VPA2 since in order to avoid generating a DTC, the difference between the VPA signals must be 0.8V +/- 0.4V. This is true regardless of any postulated faults. Additionally, VPA1 cannot short directly to the +V supply voltage, rather it must be less than 4.8V and therefore will always have an upper and lower resistance limit. This is not true for VPA2 which can fail to the +V supply voltage.

a) Simultaneous Resistive Short Faults to +V supply

For simultaneous resistive short faults to the +V supply, both the Hall Effect sensor and potentiometer sensor remain functional, therefore the effect of pressing the accelerator pedal was considered. During this postulated fault condition, the NESC team found (reference Appendix C) that if the potentiometer pedal was pressed to greater than approximately half of its full stroke then a DTC would be generated. In order to avoid generating a DTC after the simultaneous fault one of two cases must occur. If the pedal is released, the driver must not press the potentiometer pedal greater than half of the pedal’s stroke, or if it is depressed, the driver must remove his foot from the pedal within 0.5 seconds of the fault occurrence.

Although the Hall Effect sensor pedals remain functional similar to the potentiometer sensor pedals with the assumed double faults, both Hall Effect sensors remain in the operational lane through the full pedal stroke. Therefore, the Hall Effect sensor pedals will not generate a DTC if the pedal is pressed after the assumed simultaneous fault of resistive shorts between the VPA signals and the +V supply. For further detail, see Appendix C.

Assuming the pedal is at the physical idle position, Figure 6.6.2.2-6 shows the necessary resistance range required for resistive shorts to the +V supply for all three pedal types which does not generate a DTC. For example, for the two simultaneous faults common to all three pedal types to occur in the upper region, the VPA1 resistance to +V supply must be between 36Ω and 200Ω, and the VPA2 resistance to +V supply must be less than or equal to approximately 34Ω. Of all the postulated simultaneous double faults, this is the only set of conditions that has a resistance range common to all three pedal types.

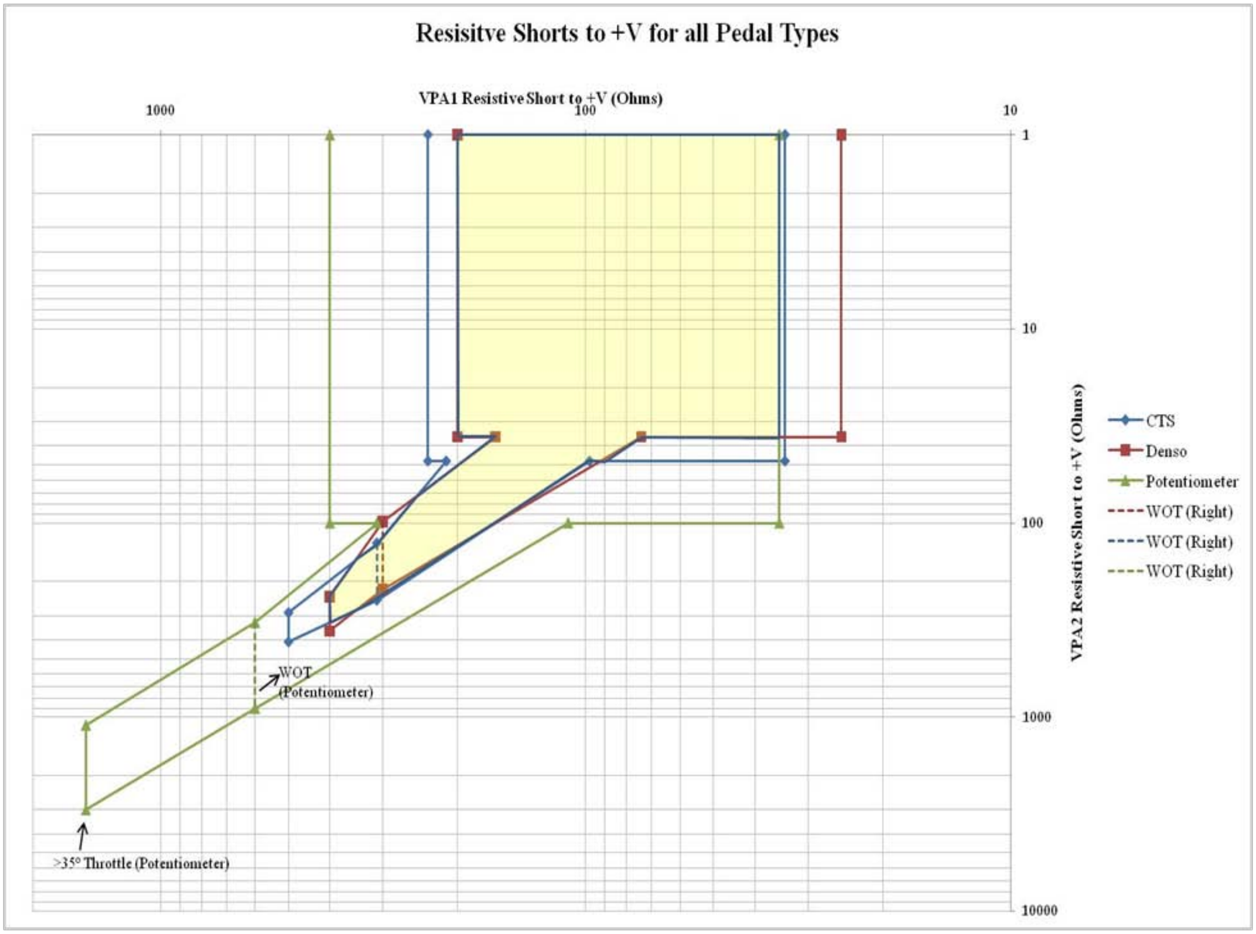


Figure 6.6.2.2-6. Resistance range required for simultaneous resistive faults between the VPA signals and the +V supply for all three pedal types. [Note: common area highlighted]

b) Simultaneous Resistive Open Circuit Faults in Return Lines

For resistive open circuit faults in the return, the potentiometer sensor remains functional and the Hall Effect sensor may remain functional, therefore again the effect of pressing the accelerator pedal was considered. The NESC team studied resistance faults with the full pedal stroke and the relationship to the operational lane was described (see Appendix C). These faults were found to remain in the operational lane.

Again, Hall Effect sensor pedals with the active amplifier output respond significantly differently to postulated subsequent resistive shorting faults to the +V supply. The NESC team studied these effects as described in Appendix C. The Hall Effect sensor signal outputs became non-operational to mechanically pressing the pedal when the return line resistance was roughly 195Ω for the Denso pedal and 650Ω for the CTS pedal.

Before relating these Hall Effect sensor responses to the operational lane, a design characteristic of the Denso pedal will be described. This design characteristic is unique to the Denso Hall Effect sensor pedals where the signal outputs are affected in a unique manner by the reduction of the sensor +V supply voltage, which was demonstrated by introducing resistance in the supply lines.

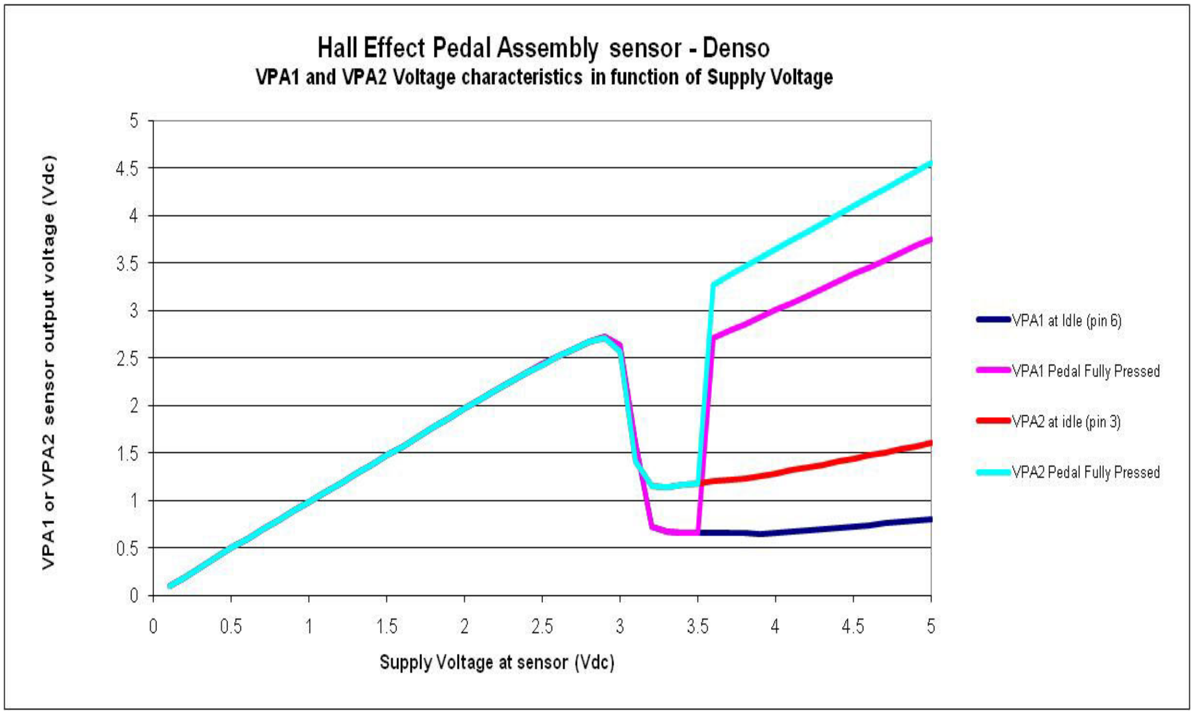


Figure 6.6.2.2-7. Denso Hall Effect sensor outputs as a function of the lower supply voltage

As shown in Figure 6.6.2.2-7, for the Denso pedal, as the supply voltages drop the output voltages also drop concurrently, however, at approximately 3V range sensor output then jumps to the supply voltage and follows the supply voltage linearly to zero. If the VPA signals converge as shown (within <0.4V) then a DTC is generated. However, depending on the fault conditions, there are voltage combinations which may put the VPA signals in the operational lane and not set a DTC. For these conditions, the Denso pedal would be subject to simultaneous dual resistive open circuit in the +V supply faults similar to the other postulated faults. However, the peak VPA signal voltage is approximately 2.7V. If VPA2 was at the maximum 2.7V, then to stay in the operational lane, then VPA1 can be no more than 2.2V or just inside the upper operational lane. This fault is similar to the postulated simultaneous resistive faults conditions in the return, but the maximum throttle opening is significantly less. Since the consequence is significantly less (just inside the upper operational lane) determining the exact resistance ranges was not explored for this unique case.

The NESC team studied (see Appendix C) two Hall Effect sensor pedals (Denso and CTS) with two examples of resistance faults, with the full pedal stoke and relationship to the operational lane described. The non-linearity of the outputs translated into cases where the VPA signals went outside the lane when the pedal was pressed for a significant portion of the pedal stroke. For the Denso pedal at the >35 degrees (absolute) throttle location, VPA2 was no longer functional, but VPA1 was still functional resulting in the pedal being outside the operational lane for the majority of the pedal stroke. The pedal outputs were non-responsive near the full throttle location resulting in the single operating point. For the CTS pedal at the >35 degrees (absolute) throttle location, the pedal was fully functional, did not go outside the lane, and at the full throttle location VPA2 was non-functional, but VPA1 was functional resulting in the pedal being outside the operational lane for over half of the pedal stroke. Therefore, if this postulated fault were to occur, then DTCs would be expected by the driver not removing their foot from the pedal within a 0.5 second of the fault occurrence.

Again, assuming the pedal is at the physical idle position, Figure 6.6.2.2-8 shows the necessary resistance range required for resistive open circuits in the VPA signal return for all three pedal types to not generate a DTC. Note that resistance ranges do not overlap and therefore there is not one set of conditions common to all pedal types which could cause a large throttle opening UA. This implies that if this postulated fault was occurring, then the conditions in addition to the other restrictions previously described would need to be uniquely tailored for each pedal type rather than common across all pedal types to avoid generating DTCs.

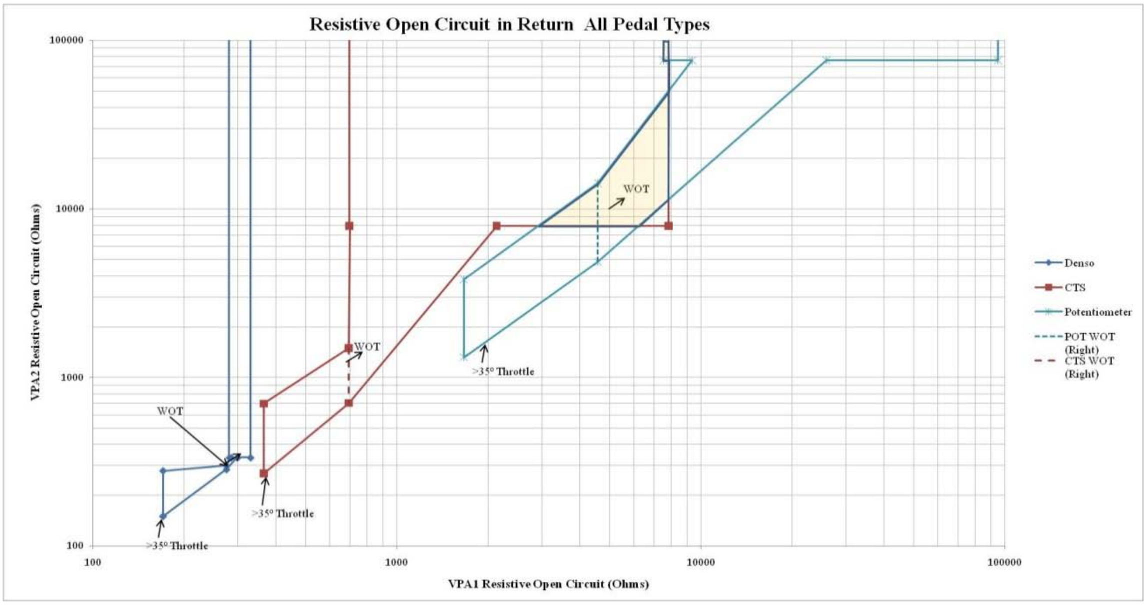


Figure 6.6.2.2-8. Resistance range required for simultaneous resistive open circuit in the VPA return line for all three pedal types

6.6.2.2.2.3 Summary of Dual faults placing the VPA signals in the operational lane:

Dual faults can be engineered to place the VPA signals in the upper operational lane, which would appear as a valid pedal command resulting in a UA. Table 6.6.2.2-1 summarizes the double faults placing the VPA signals in the operational lane.

Table 6.6.2.2-1. Summary of Dual Fault Conditions

Postulated Faults	**Resistance Range with no DTC and is it common?****			**"Allowable or Possible" Circuit Configurations & Required Sequence**		**With BOTH faults present, can a DTC be generated by pressing the pedal?**		
	CTS Hall Effect	Denso Hall Effect	Potentiometer	Hall Effect	Potentiometer	CTS Hall Effect	Denso Hall Effect	Potentiometer
Simultaneous double resistive short of VPA signals to +V	See Figure 6.6.2.2-6. Yes, there is a common resistance range for all three			2 occurrences of "2 of 21" circuit configurations*** within 0.5 sec	2 occurrences of "2 of 21" circuit configurations within 0.5 sec	NO	NO	YES
Simultaneous double resistive open of VPA signal returns	See Figure 6.6.2.2-8 Yes. small overlapping resistance range between CTS and Potentiometer		NO	2 occurrences of "2 of 21" circuit configurations within 0.5 sec	2 occurrences of "2 of 21" circuit configurations within 0.5 sec	YES	YES	NO
Latent resistance between VPA signals plus resistive short of VPA2 to +V	See Figure 6.6.2.2-5 Yes. Small overlapping resistance range		Does not apply	1st fault "1 of 21" circuit configuration followed by 2nd fault "2 of 21" circuit configurations	Does not apply	YES	YES	YES
Latent resistance between VPA signals plus resistive open of VPA2 return	~170Ω latent plus VPA2 >800Ω	130Ω < R-latent < 160Ω Plus VPA2 open > 8000Ω	Does not apply	1st fault "1 of 21" circuit configuration followed by 2nd fault "2 of 20" circuit configurations	Does not apply	YES	NO	YES

**This table does not include fault scenarios outside the operational lane, but inside the wider learning lane where DTCs are reset either through the OBDII connector or by disconnecting the battery.

***See item 2 below for description of the 21 possible circuit configurations.

The postulated faults require all four conditions to be met:

1. The two resistive faults fall in the necessary resistance range

The upper operational lane (above 35 degrees (absolute) throttle opening) represents roughly 7 percent of all possible combination of VPA signals, accounting for the lower lane of roughly equal size. This leaves 86 percent of the possible combinations of VPA signals which would generate a DTC. Tin whiskers, natural contamination or corrosion-induced faults tend to have a distribution of resistance and it would be expected to have more cases where the VPA signals occurred in the larger DTC area (86 percent). The simultaneous double resistive short of VPA signals to +V supply was the only postulated failure mode that had a common resistance range for all three pedal types.

2. The two faults build the necessary circuit configuration

There are 6 signals of interest in the pedal subsystem: 2 power lines, 2 VPA signals, and 2 returns. Assuming a simple single fault, there are 6 possible open circuit configurations plus 15 possible “one to one” shorting combinations. Therefore, there is a total of 21 possible circuit configurations in the pedal signals for a simple single fault. For the majority of the postulated faults, there are only 2 allowable circuit configurations of the 21 possible circuit configurations *which must occur twice* to place the VPA signal in the upper operational lane. A DTC would be generated if either one of the faults create one of the other possible circuits.

3. The two faults met the necessary sequence and time constraints

The latent fault was of interest because it allowed the first fault to reach the necessary resistance. The latent fault between VPA signals can decrease in resistance; however the resistance must decrease to at least 200Ω, but cannot decrease below 130Ω for the Denso pedal or 170Ω for the CTS pedal. For a UA condition, the latent fault may decrease in resistance over time, while in the precise resistance range, and then the second VPA2 fault must occur. The second fault occurring first or prior to the latent fault reaching the necessary narrow range will result in generating a DTC. These type latent faults are only applicable to vehicles using the Hall Effect sensors since potentiometer type sensors will generate a DTC with this failure mechanism.

The simultaneous double faults required the resistance faults to occur within 500 ms. A single fault or a double fault greater than 500 ms apart will generate a DTC.

It was not possible to determine which condition would be more or less probable between a double fault within 500 ms or a decreasing resistance reaching the precise range, then always followed by a second fault.

4. The pedal returns to the idle position within a 500 milliseconds.

It is not possible to determine the state of the pedal position at the time of these postulated faults. However it was possible to determine that in the presence of postulated faults that in the majority of the cases (8 of the 12 postulated failure modes, or 67 percent) the pedal was still functional and pressing the pedal could result in the VPA signals going outside the lane thus setting a DTC as discussed in Appendix C. This imposes a forth condition that the driver must allow the pedal to return to the idle position within a 500 ms. Failure to meet this condition will result in generating a DTC for some postulated faults for some positions of the pedal stroke.

Postulated faults can be engineered in the accelerator pedal signals that could result in throttle opening up to and including a WOT. Two failures in the precise resistance range, to the exact circuit configuration, in the correct time phase and the pedal not being pressed are necessary for this functional failure to occur. Failure to meet *any* one of these four specific conditions would be a “near miss” and result in generating a DTC. If these faults were occurring in normal operation, then one would expect a far more occurrences of “near misses” resulting in generating a DTC caused by:

- Fault resistance values creating voltages which fall in the larger 86 percent DTC area.
- Faults creating one of the circuit configurations which generate a DTC.
- Single faults or dual faults greater than 500 ms apart generating a DTC.
- Latent faults with the second fault too early or too late generating a DTC.
- Drivers not allowing the pedal stroke to return to idle within the 500 ms to generate a DTC.

If electronics were the cause, then it would be expected to have far more DTCs set by single faults, than by dual faults. There are 348 pedal and ECM-related DTCs (1120, 1121 and 2121), as shown in Table 6.2.5-1, and 540 VOQs which might be caused by electronics, as described in Section 6.2.4. While not proof, warranty data does not indicate an elevated occurrence of pedal or ECM-related DTCs with respect to the number of VOQs.

6.6.2.3 Evaluation of Consumer VOQ #10304368

In general, the NESC assessment focused on failures that would not generate a DTC. However, while reviewing the VOQ data, the NASA and NHTSA teams encountered a VOQ (NHTSA VOQ #10304368) related to a defective potentiometer accelerator pedal, where the consumer stated that she still possessed the defective assembly. After contacting the consumer, NHTSA was able to obtain the defective pedal for analysis. The NESC team was able to inspect, analyze, simulate and test the defective potentiometer (resistive) accelerator. The investigation revealed a resistive short between the sensor outputs (between VPA1 and VPA2) and an unexpected (not as described by the manufacturer) ETCS-i response under some system conditions. Further investigation of the accelerator pedal revealed the cause of the pedal resistive short as a tin whisker. This section describes the team’s activities associated with this particular defective accelerator pedal.

External visual, mechanical and electrical inspection of the defective accelerator pedal assembly:

a. Visual inspection of the pedal assembly showed normal wear and tear (dirt on pedal surface), but no visual damage to the unit. The connector interface was relatively clean with no visual debris.

b. Mechanical operation was verified and found to be normal. No electromechanical intermittence was observed (see system electrical test below).

c. The electrical characteristics of the defective pedal revealed a 248 ohm resistive short between the VPA1 and VPA2 sensor outputs, compromising the isolation between both sensors. Table 6.6.2.3-1 shows the resistance values obtained during the electrical tests of the defective pedal and two other “good working pedals”. Figure 6.6.2.3-1 describes the electrical configuration of the pedal with the suspected fault. All potentiometer resistances were found to be within nominal ranges, with the exception of the output isolation between each sensor as previously stated. The initial value of the isolation resistance was found to be approximately 3.5 megohms, but while handling the unit, the resistance began to decrease, first to about 5 Kohms and finally stabilizing between 250 and 238 ohms. This resistance was observed through the entire travel of the pedal (from idle to fully pressed). Also RVPA1 and RVPA2 were found to be essentially constant through the pedal stroke due to a layer of metal by design under each inner resistive half-ring which does not exist for the outer resistive half-rings.

Figure 6.2.2.3-1 is the configuration of the potentiometer accelerator pedal assembly.

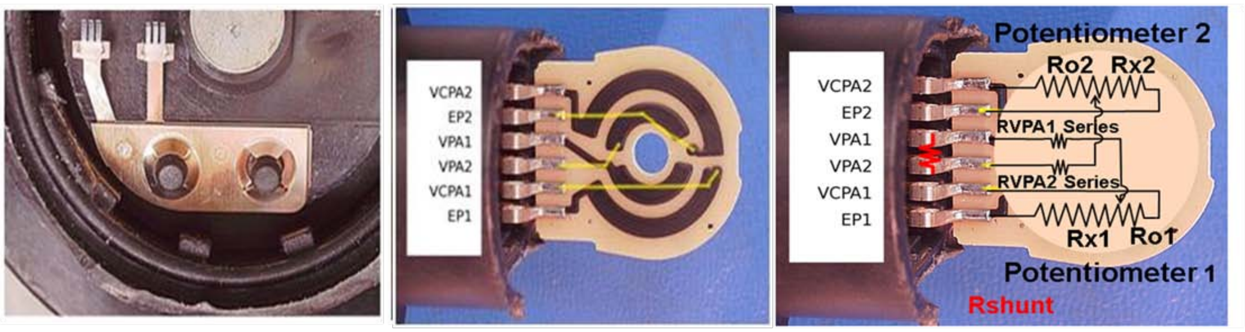


Figure 6.6.2.3-1. One of two rotating contact assemblies (left), resistive elements (center), and electrical diagram (right) for the potentiometer pedal sensors showing defective accelerator pedal assembly fault region

Table 6.6.2.3-1. Potentiometer Accelerator Pedal Assembly Resistances

		Complaint Pedal Assembly		V6 MY2006Simulator APA		L4 MY2005 Simulator APA	
		VPA Sensor n = 1	VPA2 Sensor n = 2	VPA Sensor n = 1	VPA2 Sensor n = 2	VPA Sensor n = 1	VPA2 Sensor n = 2
Measured Resistances (Ohms)	Ro"n" + Rx"n"	3480	3363	4130	4265	3389	3292
	Ro"n" + RVPA"n"	3080	2458	3663	3109	2965	2403
	Rx"n" + RVPA"n"	686	1149	777	1447	632	1091
	Rshunt	248		Open Circuit		Open Circuit	
Calculated Resistances (Ohms)	Ro"n"	2937	2336	3508	2963.5	2861	2302
	RVPA"n"	143	122	155	145.5	104	101
	Rx"n"	543	1027	622	1301.5	528	990

APA = Accelerator Pedal Assembly

6.6.2.3.1 System Behavior

Testing with a simulated defective pedal on both the V6 MY 2006 and L4 MY 2005 ETC simulators showed different responses depending on when the failure was introduced, and the number of ignition and drive cycles. The event sequence diagram, shown in Figure 6.6.2.3-2, illustrates the various responses to different operational sequences.

The first path of the event sequence diagram introduces the resistive short while driving, a DTC is declared along with a MIL, and fail-safe limp home mode is active including throttle brake override capability irrespective of the accelerator pedal position.

The second path shows after an ignition key cycle the DTC and MIL remain; however, the vehicle responds differently depending on how the accelerator is pressed. When the accelerator is pushed slowly, the vehicle has a jumpy response, and is capable of full throttle without throttle brake override. When the accelerator pedal is pushed quickly, the fail-safe limp home mode is active including brake override.

After the third ignition / drive cycle the MIL turns off, the DTC remains stored with throttle response depending on pedal application as described above.

After the battery is disconnected and then reconnected or the DTCs are otherwise cleared, the DTC and MIL does not return with throttle response depending on pedal application as described above.

As shown on the 5th path, if the resistive short occurs while the vehicle is off, starting the vehicle with the accelerator pedal partially depressed will not set a DTC. The accelerator responds as described above.

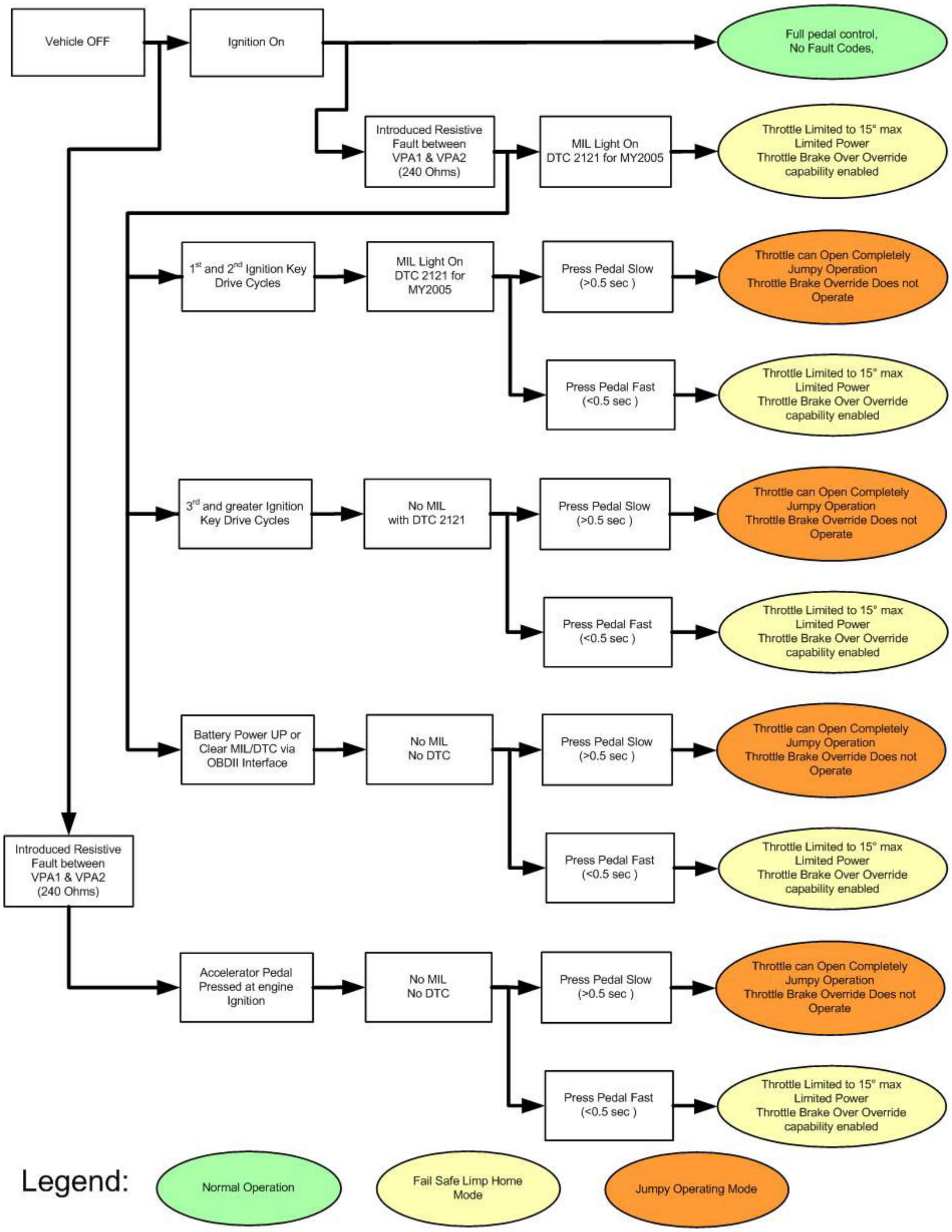

Vehicle OFF
Ignition On
Full pedal control,
No Fault Codes,
Introduced Resistive Fault between VPA1 & VPA2 (240 Ohms)
MIL Light On DTC 2121 for MY2005
Throttle Limited to 15° max
Limited Power
Throttle Brake Over Override capability enabled
1st and 2nd Ignition Key Drive Cycles
MIL Light On DTC 2121 for MY2005
Press Pedal Slow (>0.5 sec)
Throttle can Open Completely
Jumpy Operation
Throttle Brake Override Does not Operate
Press Pedal Fast (<0.5 sec)
Throttle Limited to 15° max
Limited Power
Throttle Brake Over Override capability enabled
3rd and greater Ignition Key Drive Cycles
No MIL with DTC 2121
Press Pedal Slow (>0.5 sec)
Throttle can Open Completely
Jumpy Operation
Throttle Brake Override Does not Operate
Press Pedal Fast (<0.5 sec)
Throttle Limited to 15° max
Limited Power
Throttle Brake Over Override capability enabled
Battery Power UP or Clear MIL/DTC via OBDII Interface
No MIL
No DTC
Press Pedal Slow (>0.5 sec)
Throttle can Open Completely
Jumpy Operation
Throttle Brake Override Does not Operate
Press Pedal Fast (<0.5 sec)
Throttle Limited to 15° max
Limited Power
Throttle Brake Over Override capability enabled
Introduced Resistive Fault between VPA1 & VPA2 (240 Ohms)
Accelerator Pedal Pressed at engine Ignition
No MIL
No DTC
Press Pedal Slow (>0.5 sec)
Throttle can Open Completely
Jumpy Operation
Throttle Brake Override Does not Operate
Press Pedal Fast (<0.5 sec)
Throttle Limited to 15° max
Limited Power
Throttle Brake Over Override capability enabled
Legend:
Normal Operation
Fail Safe Limp Home Mode
Jumpy Operating Mode

Figure 6.6.2.3-2. Pedal Resistive Fault Event Sequence Diagram

The following plot, Figure 6.6.2.3-3., was generated from tests performed on the MY 2006 V6 ETC simulator. A short of 248 ohms was introduced between VPA1 and VPA2.

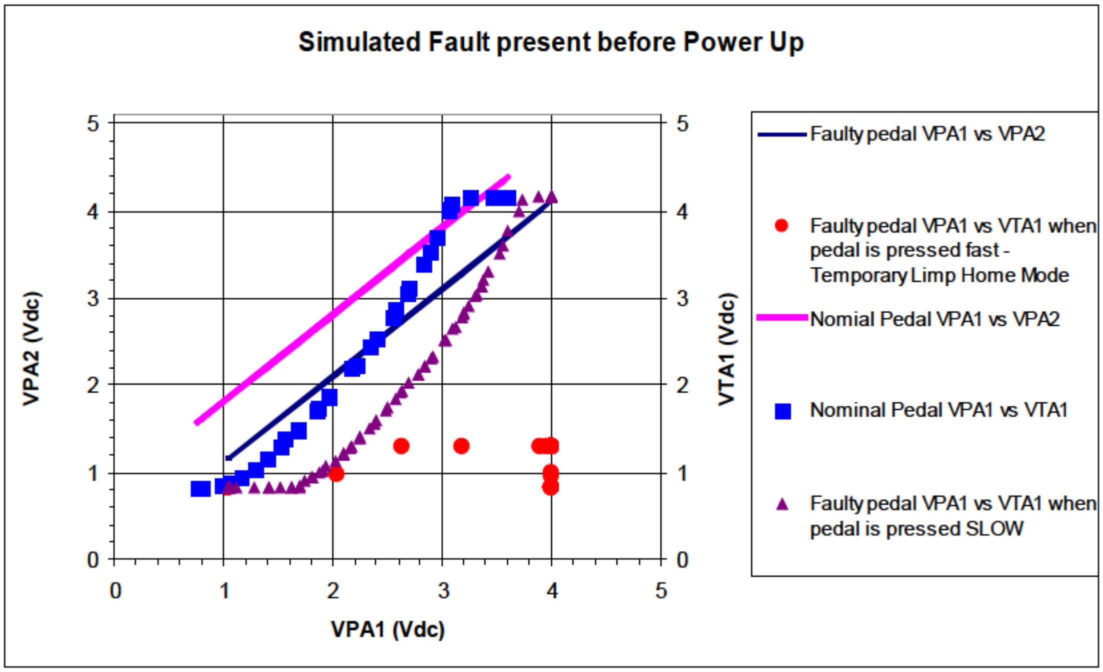


Figure 6.6.2.3-3. Simulated Pedal Fault Behavior

The nominal pedal relationship between VPA1 and VPA2 is depicted in pink. The pedal relationship with the 248 ohm short is offset below and to the right in dark blue.

The nominal relationship between pedal press (VPA1) and throttle valve position (VTA1) is depicted as blue-box data points. A smooth transition occurs at minimal pedal inputs, then increases to a maximum limit where the throttle opening no longer increases.

If the 248 ohms fault occurs after the system is powered up, a limp home mode will govern the throttle operation, thus limiting the throttle opening as described by the red dot curve of Figure 6.6.2.3-3. The throttle opens smoothly and is limited to approximately 15 degrees above idle. Also noted is the throttle closing as the throttle brake override activates when the brake pedal was applied after the pedal reached its fully pressed position.

When the 248 ohm fault already exists (between VPA1 and VPA2 at ignition turn on, the relationship between pedal press (VPA1) and throttle valve position (VTA1) is altered. And the behavior differs between a fast pedal press and a slow pedal press.

When the pedal is pressed rapidly, less than 0.5 seconds through the first 0.5 inches of pedal travel, a limp home mode is entered. This is depicted in red dots. The throttle valve opening is limited. It opens smoothly during the initial pedal travel, then limits and no longer increases as the pedal is pressed.

The following plot, Figure 6.6.2.3-4, was generated from tests performed on the 2005 L4 ETC simulator. A short of 248 ohms was introduced between VPA1 and VPA2.

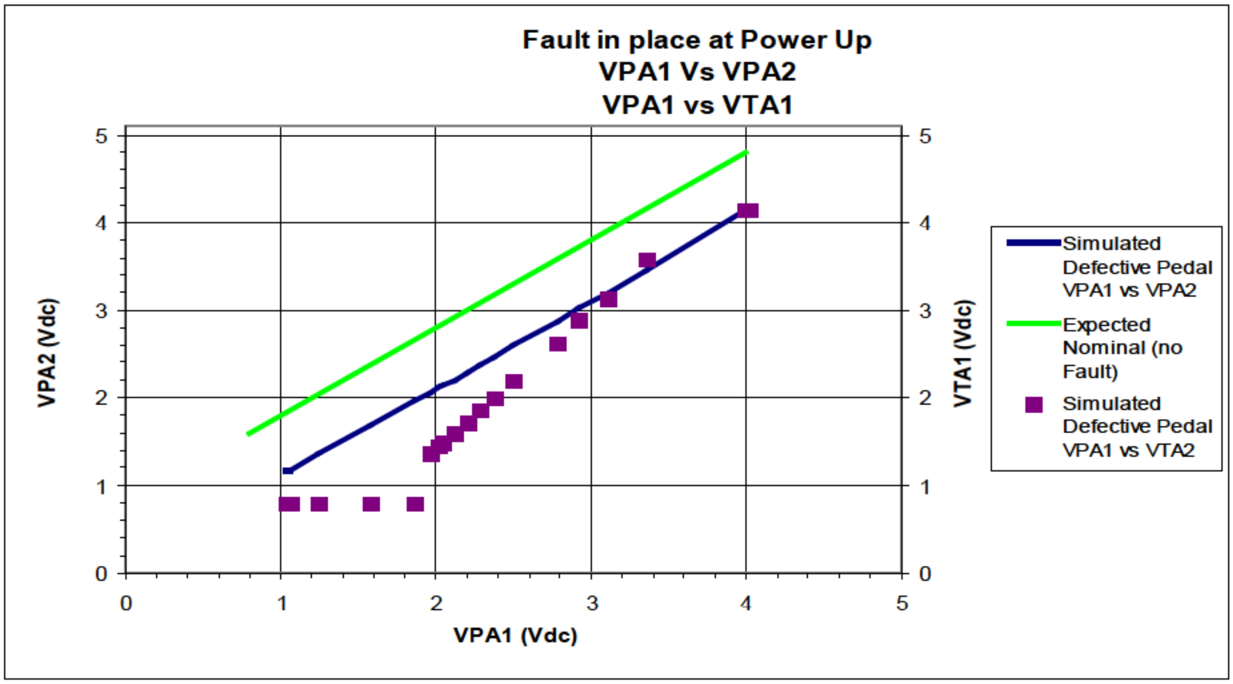


Figure 6.6.2.3-4. Fault in Place at Power Up

The nominal pedal relationship between VPA1 and VPA2 is depicted in green. The pedal relationship with the 248 ohm short is offset below and to the right in dark blue.

When the pedal is pressed slowly, more than 0.5 seconds through the first 0.5 inches of pedal travel, no throttle opening occurs during the initial pedal travel. Then a sharp increase in throttle valve opening occurs. After this sharp increase, the throttle valve can be controlled by the pedal input up to the maximum throttle valve opening, where it limits and no longer increases. This is illustrated by the purple squares. Throttle brake override capability is not available under this condition.

F-6. *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.*

a. If the resistive short occurs while the vehicle is off, starting the vehicle with the accelerator pedal partially depressed will not trigger a diagnostic trouble code. When the accelerator is pushed slowly, the vehicle has a jumpy response, and is capable of full throttle without throttle brake override. When the accelerator pedal is pushed quickly, the fail-safe limp home mode is active including brake override.

b. If the resistive short occurs while driving, a DTC is declared along with a MIL, and fail-safe limp home mode is active including throttle brake override capability.

c. If the key is cycled after the resistive short, the DTC and MIL remain. When the accelerator is pushed slowly, the vehicle has a jumpy response, and is capable of full throttle without throttle brake override. When the accelerator pedal is pushed quickly, the fail-safe limp home mode is active including brake override.

d. If the battery is disconnected with the resistive short, or the DTCs are otherwise cleared, DTCs will not return. When the accelerator is pushed slowly, the vehicle has a jumpy response and is capable of full throttle without throttle brake override. When the accelerator pedal is pushed quickly, the fail-safe limp home mode is active including throttle brake override

6.6.2.3.2 Defective Pedal Destructive Physical Analysis

Further investigation of the accelerator pedal assembly revealed the cause of the pedal resistive short.

The following images are of tin whiskers located on the faulty pedal (MY 2002 Toyota from VOQ #10304368). Tin whiskers were observed on tin-plated copper leads connecting the PCB to the pins in the housing. These are crystalline structures of tin that spontaneously may grow outward from tin-finished surfaces over time. Whisker thicknesses range from sub-µm to over 10µm and lengths vary from a few µm to millimeters. Following are images of whiskers seen on the VPA1 and VCPA1 leads as well as a characterization of the approximate (conservative) whisker length. Note that since whiskers are three-dimensional structures, only a projection of their length is visible in a two-dimensional image. VPA1 whisker ID #1 was the source of the resistive short circuit between VPA1 and VPA2. This whisker originated at VPA1 and contacted VPA2. VCPA1 whisker ID #1 was a second tin whisker of similar length which was growing from a 5V source terminal adjacent to the VPA2 signal output terminal, but had not made contact with any other terminals. Inspection of three “non-failed” potentiometer pedals revealed tin whiskers present in a similar location as the failed pedal.

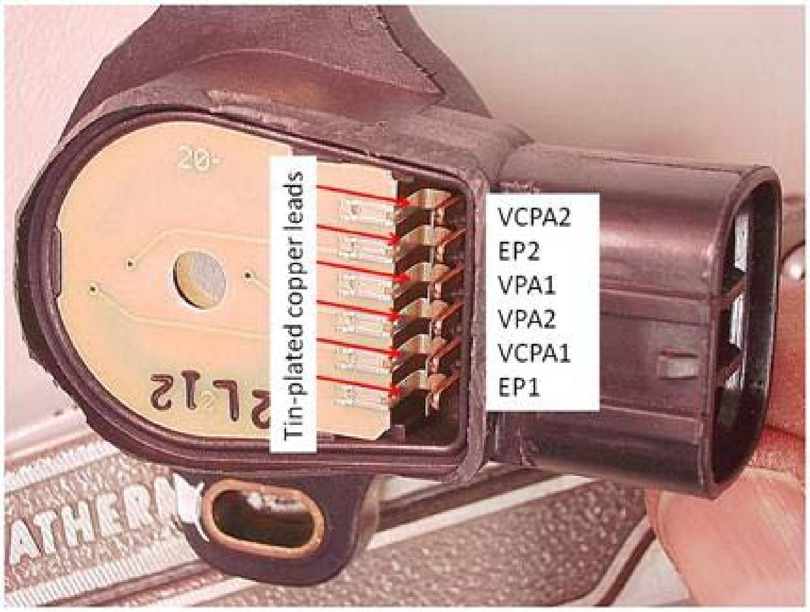


Figure 6.6.2.3-5. Disassembled Accelerator Pedal Assembly Potentiometer

Table 6.6.2.3-2. Tin Whiskers observed on the Tin-Plated Copper Leads Soldered to the PCB

Lead Name	Whisker ID #	Whisker Length Greater than (um)
EP1	1	700
EP1	2	100
EP1	3	100
VCPA1	1	1500
VCPA1	2	500
VCPA1	3	350
VCPA1	4	200
VPA2	1	300
VPA2	2	300
VPA2	3	75
VPA1	1	1900
VPA1	2	350
VPA1	3	75
EP2	1	130
VCPA2	1	200
VCPA2	2	500
VCPA2	3	500

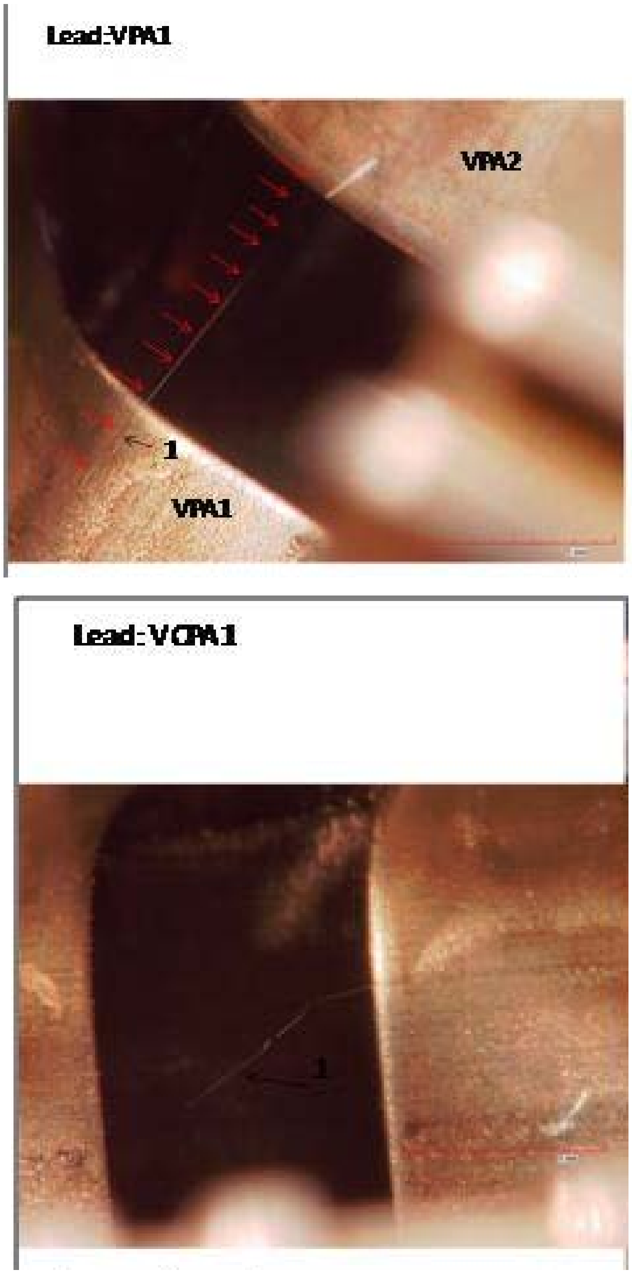


Figure 6.6.2.3-6. Shorting whisker VPA1 to VPA2 (top) and long whisker on VCPA1 (bottom)

F-5. *Destructive physical analysis of a failed pedal assembly from a VOQ vehicle with a DTC 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 additional "non-failed" potentiometer pedals revealed tin whiskers present in similar locations as the failed pedal.*

6.6.2.3.3 Tin Whisker Characteristics

This bridging whisker's thickness is calculated to be approximately 1.7 um, based on its length (1.9 mm), its electrical resistance (240 ohms), and the electrical properties of tin.

Destructive examination of two other potentiometer pedals also revealed the presence of tin whiskers in a total of three pedal assemblies: two from VOQ vehicles and one acquired from a vehicle salvage yard.

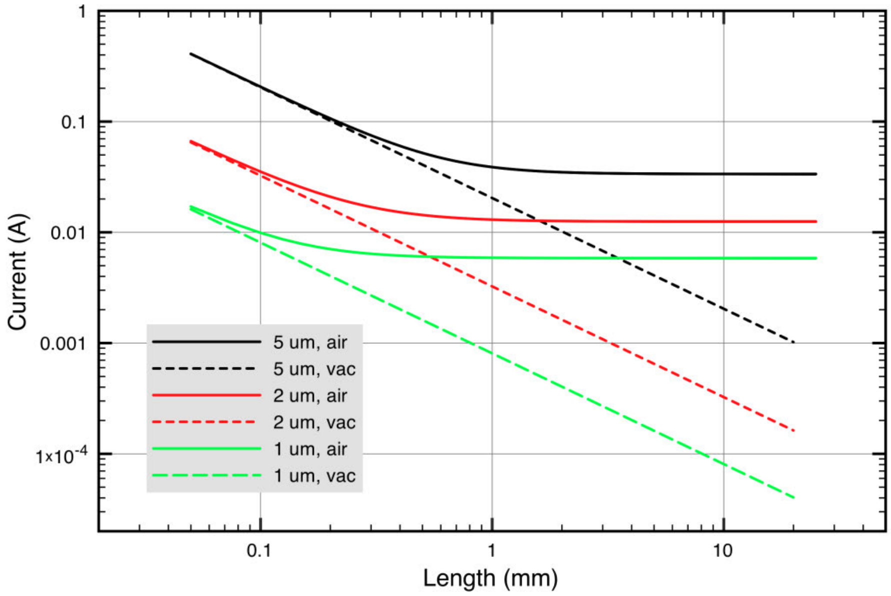


Figure 6.6.2.3-7. The current to bring a tin whisker to its melting temperature versus the length of the tin whisker[19]

[19] "Tin Whisker Initialed Vacuum Metal Arcing in Spacecraft Electronics" by James H. Richardson, Brian R. Lasley, and Capt. Theresa M. Philips, in Vacuum Metal Arcing (1992). This plot is re-drawn from their Figure 2.

The electrical current needed to melt a whisker of this length and thickness in air is approximately 5 mA, as shown in Figure 6.6.2.3-7. This current raises the temperature to the melting point of tin, 232 C, and increases the resistance of this metal whisker to about 410 ohms. The electrical characteristics of the dual potentiometer circuit cannot place such a large current through this whisker, bridging VPA1 and VPA2; thus, its survival (i.e., non-melting during the operation of the car) is expected. Electrical analysis by the NESC team determined that less than 1 mA will typically flow in a fault between VPA1 and VPA2 and a second similar fault to Vc, if it were to occur, would result in a higher current, approximately 5 ma, through that fault, but not enough to ensure melting.

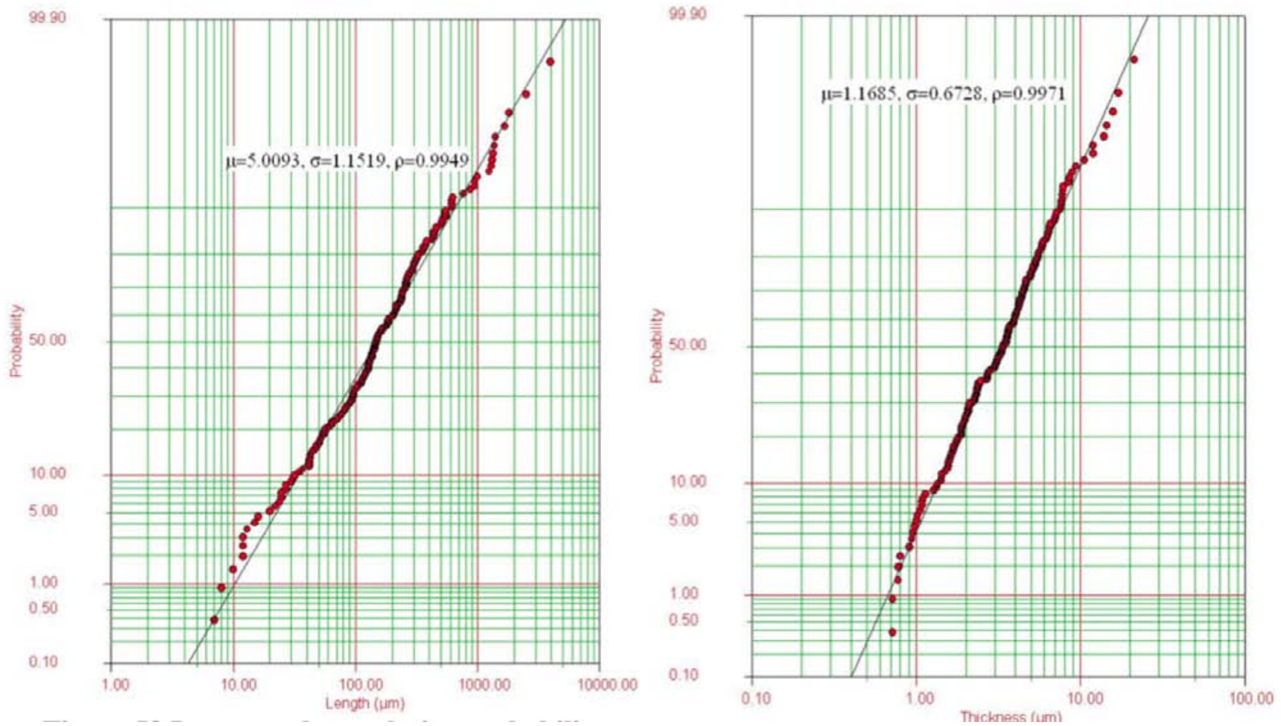


Figure 6.6.2.3-8. Lognormal cumulative probability distribution of tin whisker lengths (left) and thicknesses (right) for a sample set

The lengths and thicknesses of metal whiskers are random variables, each characterized by probability distribution functions. To date, these distributions are approximated by lognormal ones. A study[20] demonstrated that there is no correlation between length and thickness. Typical

[20] "Evaluation of Environmental Tests for Tin Whisker Assessment," Lyudmyla Panaschenko, Master's thesis, University of Maryland, 2009

results from the study are shown in Figure 6.6.2.3-8. The median length for this population is about 150 um, but about 0.5 percent is as long as 2 mm. The median thickness of this population is about 3.3 um. A whisker of thickness 1.1 um (or less) happens about 5 percent of the time. Other populations could give somewhat different values.

6.6.2.3.5 Evaluation of CTS Hall Effect Pedal Assembly

Destructive physical analysis of a CTS pedal assembly showed that the circuit card that contains the Hall Effect sensors is directly mounted to the connector as shown in Figure 6.6.2.3-9.

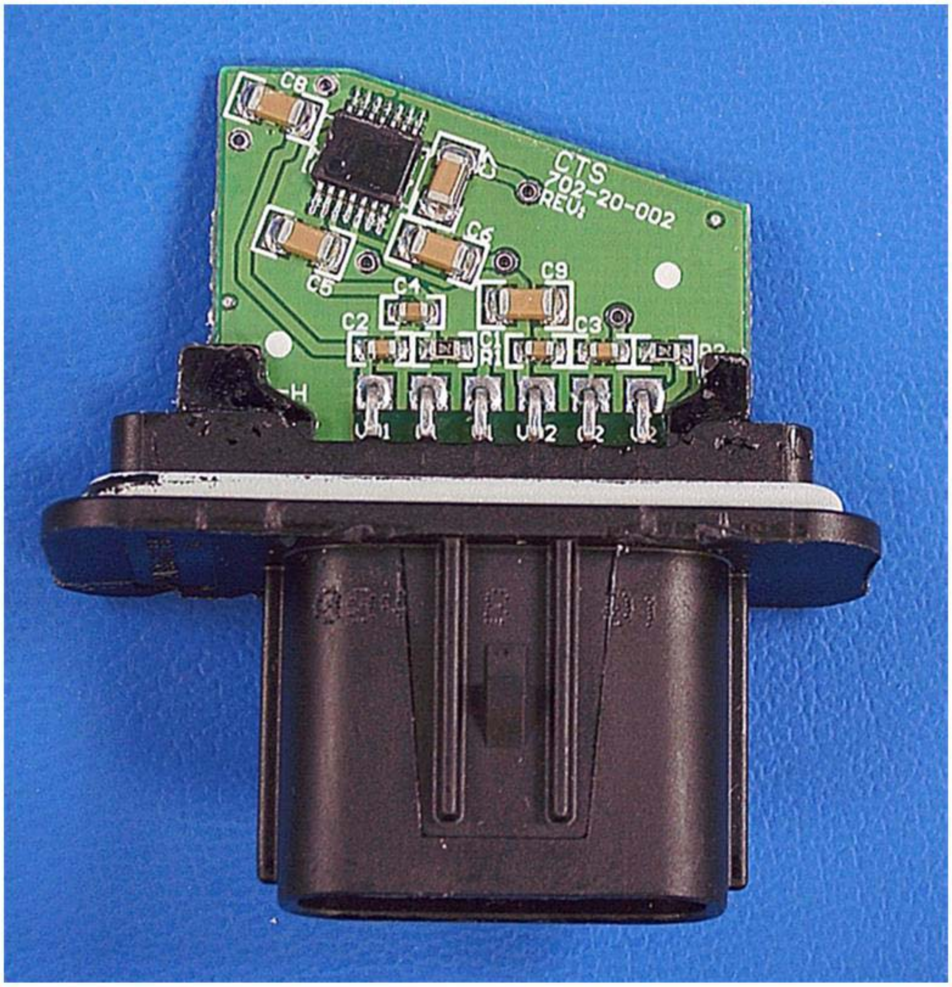


Figure 6.6.2.3-9. CTS Hall Effect Pedal Assembly Connector and Circuit Card

Figure 6.6.2.3-10 shows the CTS pedal assembly connector contact board attachment points and signal traces for VPA1 (red dots) and VPA2 (blue dots), which are physically separated. Also, the VPA1 circuit trace appears to have ground potential traces on both sides of its length. VPA2 has ground potential traces along most of its length, but there are four identified regions (green dots) where VPA2 is in proximity to +5V (VCPA1). Two of these have capacitors with tin plated end caps. A survey of solder joints showed them to be a lead/tin alloy, which is resistant to tin whisker formation. Also the circuit card has an insulating protective conformal coating over it and the parts, although some gaps in the coating were detected. The connections between the circuit card and the connector pins at the bottom of Figure 6.6.2.3-9 has pure tin, but as previously noted the VPA1 and VPA2 signals have wide separation. This configuration appears to be more robust against undesirable tin whisker shorts (particularly those between VPA1 and VPA2) than the potentiometer configuration, previously shown, where VPA1 and VPA2 pin and signal conductors are next to each other and +5V (VCPA1) is next to VPA2 with no conformal coating (see Figure 6.6.2.3-10).

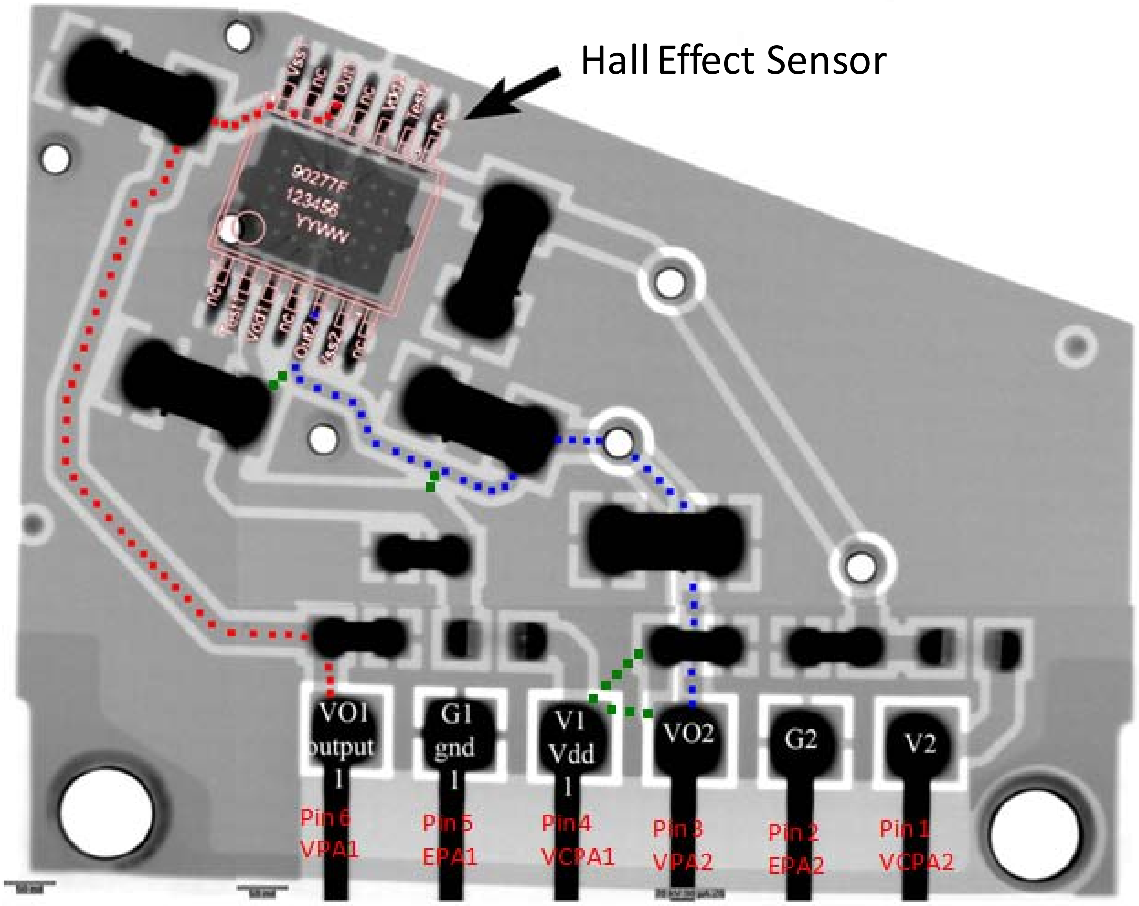


Figure 6.6.2.3-10. CTS Pedal Assembly Circuit Board X-ray Detail

6.6.2.3.6 Evaluation of Denso Hall Effect pedal assembly

X-ray and destructive physical analysis of the Denso Hall Effect Sensor provided construction details as shown in Figure 6.6.2.3-11.

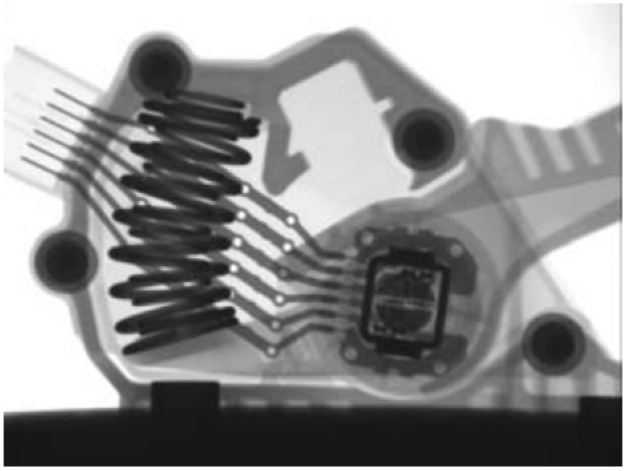


Figure 6.6.2.3-11. X-ray of Denso pedal assembly

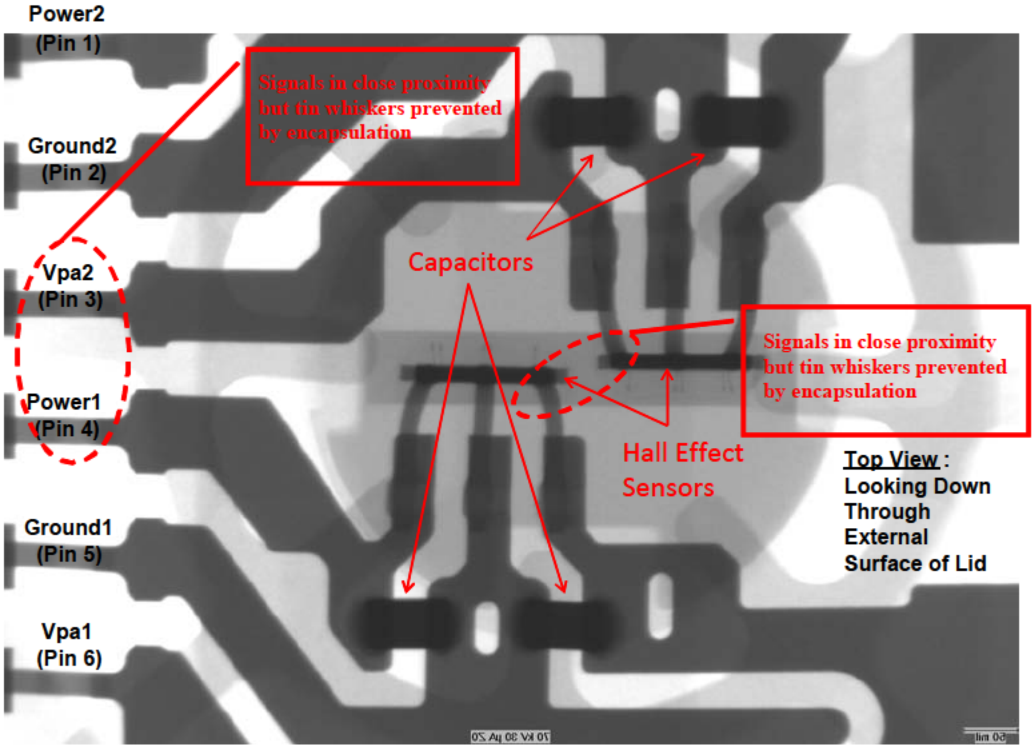

Power2
(Pin 1)
Ground2
(Pin 2)
Signals in close proximity but tin whiskers prevented by encapsulation
Vpa2
(Pin 3)
Capacitors
Power1
(Pin 4)
Signals in close proximity but tin whiskers prevented by encapsulation
Hall Effect Sensors
Top View : Looking Down Through External Surface of Lid
Ground1
(Pin 5)
Vpa1
(Pin 6)

Figure 6.6.2.3-12. Denso Pedal Assembly Circuit Board X-ray Detail

The Denso pedal assembly is a different construction than the CTS pedal. The circuit board and parts are essentially embedded in a solid plastic potting material. Therefore, although there are capacitors with the possibility of pure tin end caps and lead wires on the Hall Effect sensors which may also have tin-plated leads, the plastic material serves as a barrier against tin whisker shorting. Based on this analysis, the Denso Hall Effect pedal assembly appears to be robust against undesirable tin whisker shorting for both VPA1 to VPA2 shorts and for shorts of signal to 5V power (Vc).

While inspection of several accelerator pedal assemblies (5 Potentiometer type; 1 CTS and 1 Denso Hall Effect types) for presence or likelihood of tin whiskers was quite extensive, physical inspection on other components of the ETC was limited. The pedal signal/power circuit paths in the ECM are in an area of most interest since resistive shorts in this component would have the same effect as in the pedals. There are numerous versions (up to 4 different circuit card versions per year) of the Camry ECMs over the 8-year time period. Examination of one MY 2007 ECM concentrated on inspecting the printed circuit board, its components and its housing, for evidence or precursors that could produce electrical resistive shorts or open circuits.

The examination revealed that the solder used on the printed circuit board was a “lead free” tin alloy called Sn-Ag-Cu (“SAC”), which is less prone to formation of tin whiskers than pure tin solder. There were no traces of pure tin coating on connector pins and no solder cracks or cold solders. The examination found that the printed circuit board is not conformal coated and part of the enclosure of the ECM is made out of an aluminum-zinc alloy which can develop whiskers. However, the inspection of this ECM revealed no tin or zinc metallic whisker growth, nor precursors that sometimes predict the later growth of metal whiskers.

F-5a. *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.*

6.6.3 Idle Speed Control Functional Area

6.6.3.1 Detailed Implementation Description

The ISC loop is a feed forward control system that maintains the engine running when no driver input is present (idle) and derives engine speed from the NE+ crankshaft signal as the primary feedback control. In addition the ISC controls functions to compensate for conditions like creep control, increases in oil temperature, variable valve timing, alternator loads, air conditioner loads, catalyst temperature, idle while moving, stall prevention, electric loads other than the alternator, variations in the throttle valve assembly, emissions control system purging, power steering, startup/ignition, and engine temperature to smooth the driving experience and engine operation. The ISC throttle angle request is added to the learned throttle detent position after the throttle requests from the other ISC functions have been determined. ISC calculates the amount of air required, in gm/s, and converts this value to a throttle angle request. Within the ISC function there is a predictor function, in the form of a look-up table, which converts the amount of air to a throttle angle. This predictor function includes a learning value to compensate for deposits in the throttle assembly. The ISC contribution is comprised of three main components: 1) The ISC learning compensation, 2) the ISC target engine speed/actual speed feedback control, and 3) engine loads.

The maximum throttle angle contribution from ISC is set to 15.5 degrees by a software guard limit. Testing of the software model (258,048 iterations), showed a maximum combined effect of 11.6 degrees. The software tests indicated the engine coolant temperature sensor as having the greatest influence. Testing by failing the engine coolant temperature sensor to the lowest value of a Camry MY 2005 L4 showed a maximum of 4.2 degrees increase in throttle angle due for this single sensor failure.

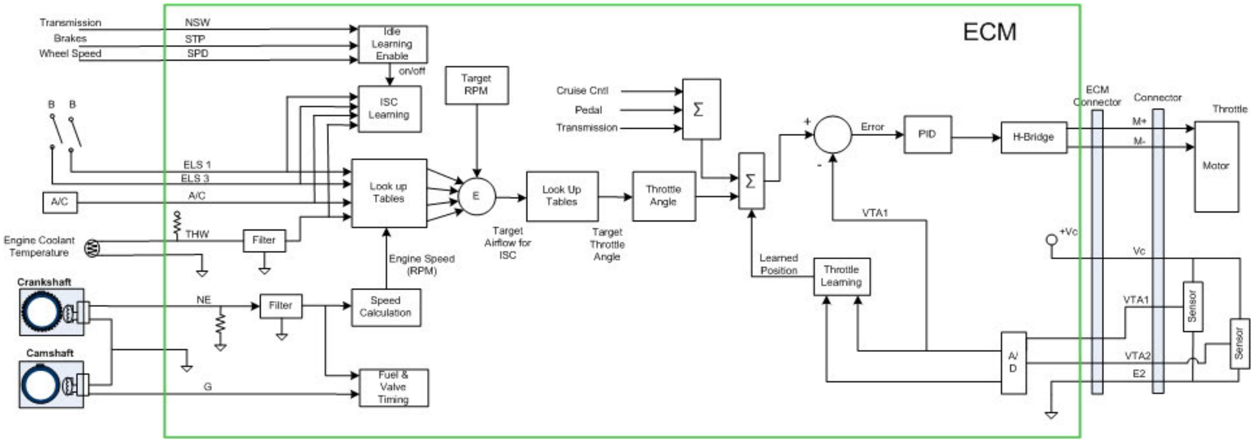


Figure 6.6.3-1. Idle Speed Control Functional Block Diagram

The accelerator pedal position, transmission position indicator, neutral switch (NSW), the vehicle speed (SPD) and the brake indicators (STP) are used to determine when the engine is idling.   The electrical load switch, the air conditioning switch and the engine coolant temperature are used to add an additional level to the target value depending on the need for increased engine speed. The crankshaft position (NE+) is used in conjunction with the camshaft position (G+) signal to set the proper timing of the engine intake/exhaust valves position and the fuel injection timing.

6.6.3.2 ISC Engine Coolant Temperature

The ISC uses the water coolant temperature (software value *ethw*) representing the measurement taken at the water temperature sensor, as an input to various software modules within the ISC to determine throttle valve angle contribution to maintain idle. Many of these calculations are done based on the measured water temperature. Operation of fuel cut is further described in section 6.7.2.7.

6.6.3.3 "Idle On" Fuel Cut Function

There is protection against excessive engine speed commanded from the ISC through the fuel cut function. The fuel cut function will engage when the engine speed reaches a threshold. The fuel cut threshold will change as a function of the engine coolant temperature.

Once fuel cut is engaged the engine speed will drop until it reaches a fuel cut disengage limit.

6.6.3.4 Idle Speed Control System Sensitivities and Postulated Faults

Figure 6.6.3.4-1 shows the summary of postulated faults identified by the fishbone for the ISC functional area. Based on the understanding of the ISC design as described, the ISC system was reviewed for sensitivities where a postulated fault could result in an increase in engine speed. The fishbone was used to identify potential sensitive entry points into the ISC loop. The fishbone identified a poor electrical connection, wiring or faulty engine coolant temperature sensor that may create the potential fault listed below. The next section details postulated faults and effects for the ISC.

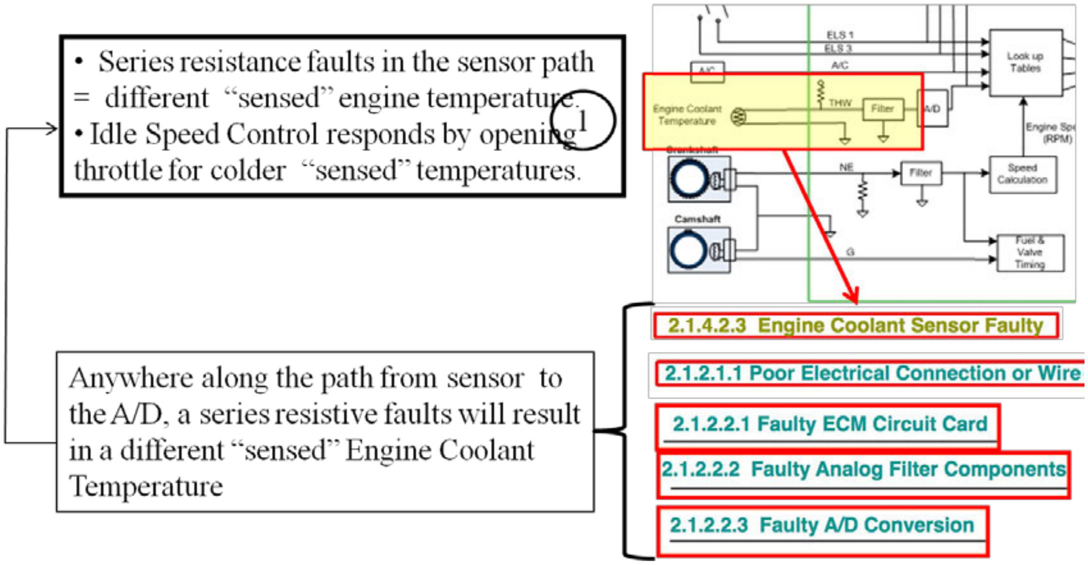

• Series resistance faults in the sensor path = different "sensed" engine temperature.
• Idle Speed Control responds by opening throttle for colder "sensed" temperatures.
1
Anywhere along the path from sensor to the A/D, a series resistive faults will result in a different "sensed" Engine Coolant Temperature
ELS 1
ELS 3
A/C
A/C
THW
Filter
A/D
Look up Tables
Engine Coolant Temperature
Engine Speed (RPM)
Crankshaft
NE
Filter
Speed Calculation
Camshaft
G
Fuel & Valve Timing
2.1.4.2.3 Engine Coolant Sensor Faulty
2.1.2.1.1 Poor Electrical Connection or Wire
2.1.2.2.1 Faulty ECM Circuit Card
2.1.2.2.2 Faulty Analog Filter Components
2.1.2.2.3 Faulty A/D Conversion

Figure 6.6.3.4-1. Summary of postulated faults identied by Idle Speed Control Function Fishbone Diagram

6.6.3.5 Engine Coolant Sensor Fault

In the ISC, the only sensor signal that produced a noticeable (2000 rpm in neutral) increase in engine speed was the coolant temperature sensor (hardware label THW) failing to a higher resistance.

6.6.3.6 Engine Speed Signals Corruption

In the ISC, the engine speed is controlled to a target engine speed, thus causing the ECM to think the engine is slower than actual should result in an increased engine speed. The testing attempted to "fool the ECM" by trying to create a slower engine speed by corrupting the engine speed feedback signal or crankshaft position (NE+) signal.

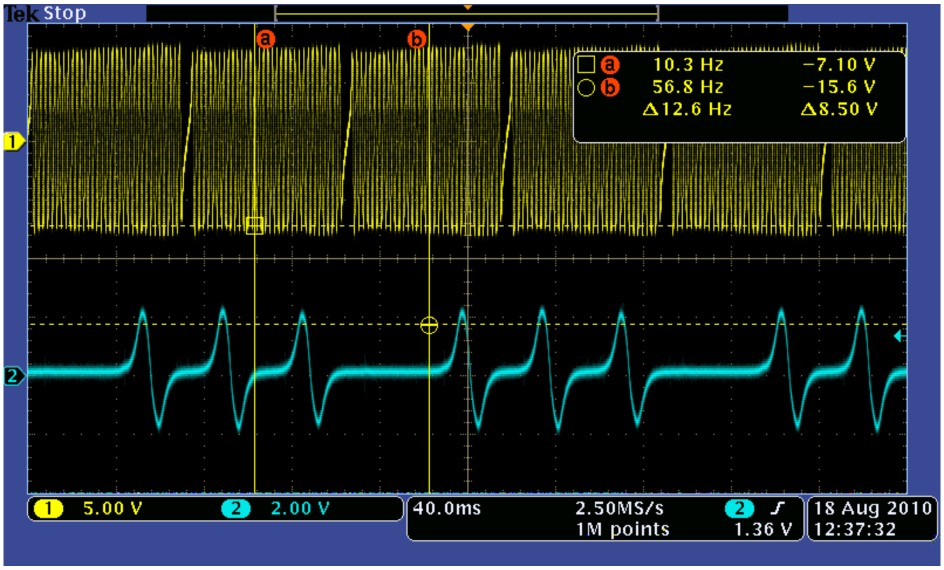


Figure 6.6.3.6-1. NE signal (Crankshaft, top yellow) and G (Camshaft, bottom blue) signal at idle

The crankshaft position (NE+) is used in conjunction with the camshaft position (G+) signal to set the proper timing of the engine intake/exhaust valves position and the fuel injection timing. Any corruption of these two signals that fails to maintain the proper timing relative to the actual engine speed will stall the engine. Therefore, the testing focused on creating small changes to the actual crankshaft sensor signals. The crankshaft signal is approximately 13V peak to peak, approximately 600 Hz at idle and increases in magnitude and frequency at higher engine speeds. The ECM converts this signal into a digital clock signal by a zero crossing detection circuit. Therefore, the zero crossing detection circuitry was tested to sensitivities to offsets. The result was that it was easy to stall the engine. No increase in engine speed was observed in the vehicle with an offset on the crankshaft signal induced by sine wave, square wave and saw tooth waveforms from 1 Hz up to approximately 90 KHz.

6.6.3.7 Failed Compensation for Additional Engine Loads

The ISC learning algorithm uses the signals listed below to determine if an increase in the target engine speed is required. These signals are for a MY 2005 Camry:

- Electronic Load Switch #1 (ELS1)
- Electronic Load Switch #3 (ELS3)
- Air Conditioning Switch (A/CS)
- Coolant Water Temperature Sensor(THW)

The electronic load switches are a binary input (ON/OFF) signals to the ECM based on the status of electrical loads that cause increased alternator loading on the engine, and testing shown no observable increase in engine speed with the vehicle in neutral. The air conditioning switch is also a binary input and testing showed a sustained ~200 increase in rpm with the vehicle in neutral. The testing involved providing the ECM with false ON when the load was not present. The engine speed increased as a result of the air conditioner cycling and is discussed in the nominal design feature (Section 6.6). The engine increase will occur coincident with the air conditioning switch state regardless if the air conditioner load is present or not.

The water coolant temperature sensor provides an analog input proportional to temperature, colder temperature is higher resistance. When the sensor has failed to a higher resistance there is a range where the engine speed will increase by 2000 rpm (vehicle in neutral) without generating a DTC. Figure 6.6.3.7-1 shows the test results for the test where the vehicle was started with the coolant temperature sensor set to ~80C, then failed to a higher temperature (130 ohms or 244F) at 30 seconds into the test then failed to a lower temperature (150 Kohms or -40F) at approximately 1 minute into the test. As shown in the block diagram, Figure 6.6.3-1, this engine speed increase is in addition to the other throttle requests.

A mapping of the coolant temperature sensor resistance to the ECM’s reported temperature through the Techstream was performed. The upper resistance range with respect to the DTC range is shown in Figure 6.6.3.7-2. As the resistance of THW sensor input increases, the ECM input approaches the upper limit of the supply voltage. The DTC occurs at 4.92V or 80mV from an ideal 5.00V supply. The return wire of the sensor has additional connections to other electronic devices in the vehicle.

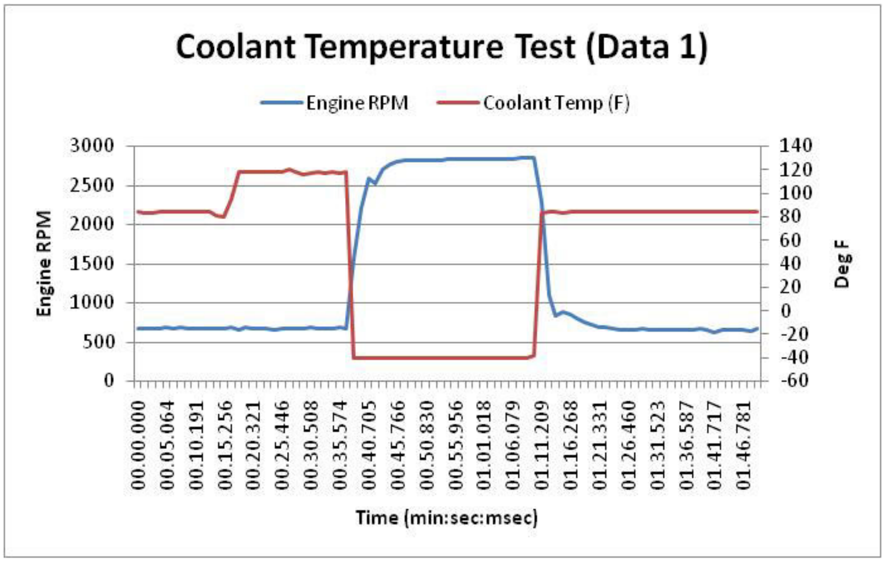


Figure 6.6.3.7-1. Test results with coolant temperature sensor failed to 150 Kohms resulting 2000 RPM increase with vehicle in neutral

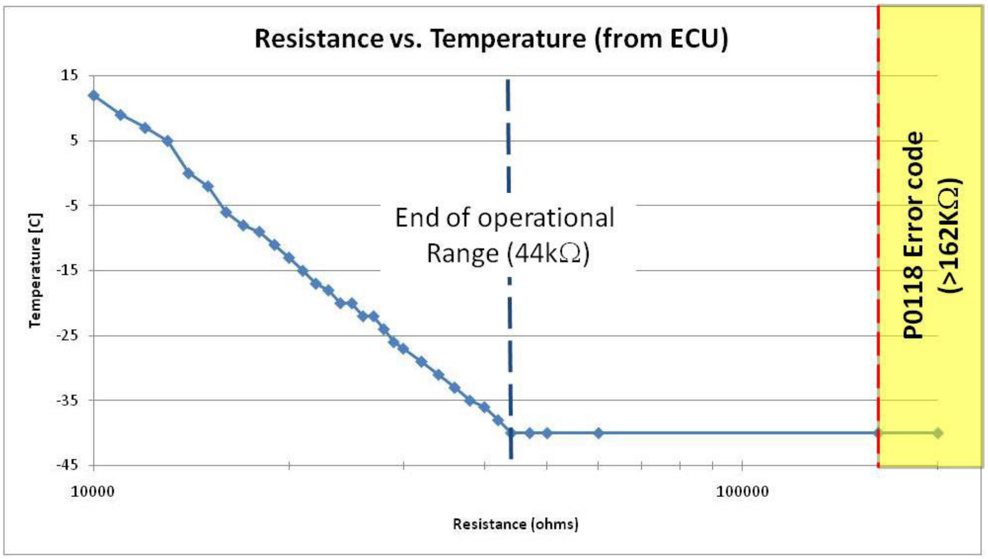


Figure 6.6.3.7-2. Upper resistance range of the Coolant Temperature Sensor including the DTC error range

For the coolant temperature sensor, the ECM software look-up table increases the target rpm directly proportional to the temperature reaching a maximum at -40C. When tested on a vehicle, the vehicle would not start when the engine was warm. Additionally, as the engine warmed the vehicle did not run smoothly, therefore the driver would have other indication the vehicle was not operating properly. These symptoms were not seen in the VOQs and there is no incidence of DTCs or repairs, therefore this postulated failure is not supported by the available data.

6.6.3.8 Summary of Idle Speed Control Potential Faults

A poor electrical connection at the coolant sensor, circuit connectors, or in the wiring, could result in an increased resistance. The fault could occur as long as the vehicle is achieving nominal operating temperature, approximately 20 minutes; however, it would eventually set a P0115 DTC. Since the water coolant sensor changed the throttle by less than 5 degrees, it would not explain the greater than 25 degrees above idle unintended throttle valve opening acceleration events.

F-8. *Functional failures of idle speed control, transmission control, VSC, and throttle control may result in throttle openings of less than 5 degrees above idle and may not generate a DTC.*

6.6.4 Cruise Control Functional Area

6.6.4.1 Detailed Implementation Description

Cruise control maintains the vehicle speed within set limits while cruising with foot off the accelerator pedal and uses the vehicle wheel speed as the primary control signal. Figure 6.6.4-1 shows the cruise control block diagram. The cruise control function is implemented through a single variable voltage input that is manipulated by the driver through a switch.

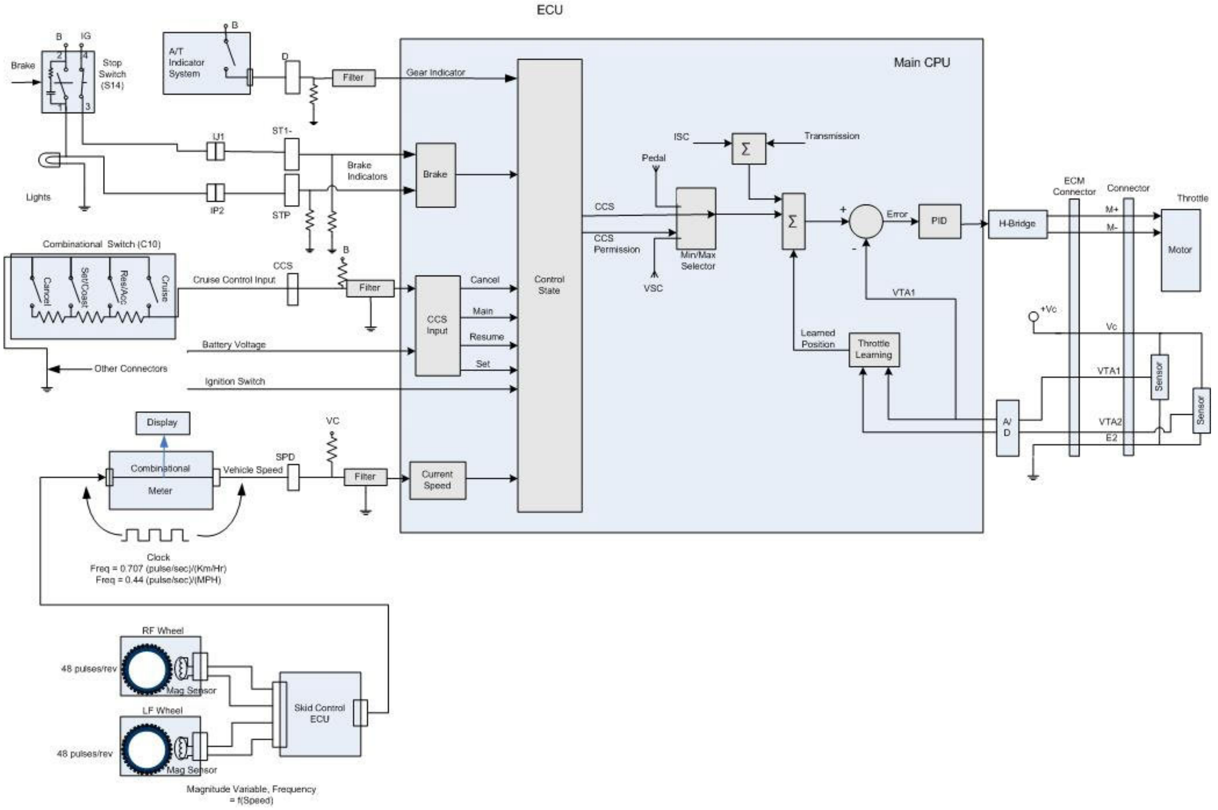


Figure 6.6.4-1. Cruise Control Block Diagram

The switch selects a resistance that is interpreted by the cruise control logic as a variable voltage that sets the state of the cruise control as shown in Table 6.6.4-1. The four switch resistors produce a voltage divider of the battery voltage that combine to represent the five cruise control switch states: Main, Resume, Set, Cancel, Off. The table below describes the conditions for setting of each of the cruise control switch states. Vehicle wheel speed is determined through a combination meter from sensors on the two front wheels. The system checks whether vehicle speed reading changes more than [redacted] percent from one reading to the next, and if so cruise control will be auto canceled. If the speed drops more than 9 mph below the set point, cruise control will auto cancel.

Table 6.6.4-1. Cruise Control Switch Voltage Output

Cruise Control Switch Voltage	Cruise Control Switch State
CC voltage (CCV) <= (0.168 * Battery Voltage(BV))	Main On/Off
(0.168 * BV) > CCV >= (0.3685 * BV)	Resume On/Off

Cruise Control Switch Voltage	Cruise Control Switch State
(0.3685 * BV) > CCV >= (0.584 * BV)	Set On/Off
(0.584 * BV) > CCV >= (0.7934 * BV)	Cancel On/Off
(0.7934 * BV) > CCV	Off

Additionally, there are noise removal functions to smooth out signal irregularities.

The actual setting of a cruise control state requires one of the cruise control switches to be pressed and then released. In software, this results in a state change being registered followed by the “Off” state. When the driver engages the cruise control switch, the switch is pushed in; this corresponds with Main, Resume, Set, or Cancel. When the driver lets off of the switch, it returns to the normal position corresponding to the “Off” state.

In addition to the cruise control states described above, there are manipulations of the same cruise control switch that allow for other states that are described in Table 6.6.4-2.

Table 6.6.4-2. Cruise Control States

Cruise Control State	Activation	Description
Coast	Set switch is engaged for longer than 0.6 seconds	While engaged, coast will decrease the speed of the vehicle. When disengaged the new vehicle speed becomes the set speed.
Tap Down	Set switch is engaged	Each time the set switch is engaged the vehicle speed will decrease by 1.6 kph and becomes the new set speed.
Accel	Resume switch is engaged for longer than 0.6 seconds	While engaged, accel will increase the speed of the vehicle. When disengaged the new vehicle speed becomes the set speed.
Tap Up	Resume switch is engaged	Each time the resume switch is engaged the vehicle speed increases by 1.6 kph and becomes the new set speed.

The cruise control operation may be manually canceled through four different inputs:

1. Cancel switch is engaged
2. Main switch is turned off
3. Brake is depressed
4. Shift from drive

Four diagnostic codes are shown in Table 6.6.4-3 that describes the cruise control failures.

Table 6.6.4-3. Cruise Control Diagnostic Codes

P0571 Brake Switch Circuit Abnormal	Checks coherency of the two brake switches.
P0500 Vehicle Speed Sensor Abnormal	Checks whether a speed pulse is registered by the vehicle within 140 seconds of ignition on.
P0503 Vehicle Speed Sensor Intermittent/Erratic/High	Checks whether vehicle speed reading changes more than [redacted] percent from one reading to the next.
P0607 Cancellation Circuit Abnormal	Checks various voltages, data mirrored in RAM, and brake switch state. Voltages checked include +B low voltage, ignition switch low voltage, watchdog interrupt (WI) low voltage, and STA low voltage.

Auto cancel refers to the function of automatically canceling the cruise control set speed because of certain conditions or diagnostic outputs. There are three subsets of auto cancel described in Table 6.6.4-4.

Table 6.6.4-4. Cruise Control Auto Cancel

Low Speed	Cancels when the vehicle speed is less than 36 kph, or 16 kph below the set speed.
Diagnostics(No code)	Cancels when there is an abnormality detected in the electronic throttle or there is a contradiction in the two accelerator pedal position sensors, or there is an abnormality in the intake air mass flow valve or if the data mirrored in RAM is not nominal.
Diagnostics(P0571, P0500, P0503, P0607)	Cancels if any of the following DTCs occur: (P0571, P0500, P0503, P0607).

6.6.4.2 Cruise Control System Sensitivities and Postulated Faults

The software study focused on the following:

1. Failure modes of the cruise control switch that causes an acceleration behavior and no DTC or indication.
2. Failure modes that prevent the cruise control from being reset or cancelled.
3. Failure of the speed sensors.

As a result of the software study, focused areas for hardware testing were selected for vehicle tests. The following summarizes several tests performed on a MY 2005 Camry at the VRTC.

6.6.4.3 Vehicle Test: Enable Cruise Control and Restrain Brake Switch Plunger

The brake switch consists of one normally-open switch and one normally-closed switch. Both are mechanically connected with a switch plunger.

With the cruise control enabled and the brake switch plunger disabled, the cruise control remained activated and functioning even when brake pedal applications were induced. The system maintained the set speed until enough brake force was applied to decrease vehicle speed by approximately 9 mph or below the 25 mph threshold of operation causing the system to fully disengage. No DTC was generated.

6.6.4.4 Vehicle Test: Short Cruise Control Signal Resistively to Ground

With the cruise control engaged, a 240 Ohm resistive short of the cruise control signal wire to ground caused the cruise control to remain engaged and the vehicle accelerated to the maximum speed threshold of the system. This test simulated the ACCEL button in a failed closed position. If the brake pedal was applied with the short present, the system canceled. After releasing the brake pedal, if the short is recycled, the system would resume to the previously set speed, and can be canceled again by pressing the brake.

6.6.4.5 Vehicle Test: Cruise Control shift out of drive cancel

With the cruise control enabled, the system canceled when the transmission was manually downshifted or shifted to neutral. The system could be resumed to the previously set speed when the transmission was placed back in Drive and the resume button was depressed.

6.6.4.6 Failed Wheel speed sensor

If a fault in the vehicle speed determination indicates a lower speed than the vehicle, the cruise control function will increase the throttle to increase vehicle speed. Signal Line and Voltage Ripple tests were performed during EMI Conducted Susceptibility tests, Section 6.8, with no effect seen on the vehicle speed control when in cruise control.

***F-7**. Functional failures of the cruise control can result in 0.06 g's acceleration, or 2.12 kph/s, and may not generate a DTC; however, there are multiple methods for cancelling or turning off cruise control.*

6.6.5 Transmission Control Functional Area

The ETCS-i uses a transmission shifting signal as an input to its determination of throttle command. The transmission control software has a hard limit of 5 degrees to the throttle command. The only area evaluated for effect on ETCS-i was torque converter lock-up, and the acceleration was determined to be minimal. The torque converter converts the power from the engine seamlessly to the transmission. In order to improve fuel economy, the torque converter is equipped with a lock-up clutch, which locks as the vehicle speed reaches approximately 40 mph. This lock-up is controlled by the CPU and engages in the top gears, and will disengage with changes in accelerator pedal movement.

6.6.6 VSC Functional Area

VSC primary function is to keep the vehicle in a correct attitude or orientation on the road. Traction Control (TRAC) is contained within the VSC function and is intended to keep the difference between the drive wheels' speed and the vehicle speed minimal to control wheel slip during accelerator pedal application. The stability control will cause the vehicle to brake and decrease the throttle angle if the actual vehicle yaw rate varies from the commanded vehicle yaw rate. The commanded yaw rate as based on the steering wheel and the vehicle yaw rate is sensed from 2 microelectromechanical systems (MEMS) gyros. The braking request from the stability control will also cancel cruise control, if it is active.

MY05 does not increase throttle through VSC. If a speed sensor fails, then the VSC function will stop (DTCs C0200, C0205, C0210, and C0215). The drive wheel speed is averaged between the values of the two front wheel speeds.

DTCs for the two front wheels (C0200 and C0205) check whether a speed sensor pulse has been received after 0.04 seconds. These DTCs are only checked if the vehicle speed is greater than 25 mph.

The ability of VSC to increase the throttle was discussed with the TMC engineers, but not studied in great detail. The VSC was optional up to MY 2010 and, based on the discussions, does not have the ability to increase the throttle up to MY 2007.

6.6.7 ECM Power System

Although not a functional control loop related to vehicle operations directly, electrical power is necessary for the control loops to function properly, therefore just as important as any control loop. A thorough review of the power system did not identify any failure modes which would result in a throttle increase other than the modes already identified as influences to the major control loops.

6.6.7.1 Detailed Implementation Description

Figure 6.6.7-1 is a simplified diagram of the power supply ASIC used in the MY 2005 Camry L4.

[redacted]

[redacted]

[redacted] The Vc supply regulator has foldback current limiting that limits the current into an external short circuit to approximately 520 mA which was verified by NESC testing. The Vc is also used outside the ECM to power the throttle and pedal position sensors and other vehicle sensors in addition to circuitry inside the ECM. [redacted].

6.6.7.2 Power System Sensitivities and Postulated Faults

There are no identified single point failures in the power supply that can trigger a vehicle UA. [redacted] Lastly, since the Vc output is used to power various sensors in the vehicle a short of this +5V line to the battery voltage may be possible. This was tested on a MY 06 V6 simulator by gradually shorting the external Vc to the +12V source through a variable resistance. At a voltage greater than approximately 8V the ECM became non-functional and permanently damaged (Vc decreased to approximately 2.5V), but no unexpected opening of the throttle was observed. EMI testing audio ripple and spikes were injected on both the +12V and +5V Vc lines at the ECM and no UA was reported. Low voltage output of a single regulator should cause ECM anomalies that can be detected by DTCs. Lastly, open output capacitors may result in increased power supply noise and/or oscillation. The previously noted ripple injection tests for the ECM +12V and +5V Vc lines were performed without UA incident. The undervoltage detection circuits previously described protect the system against low Vc voltage and low +12V affecting the CPUs and other electronics.

6.7 Software Analysis

6.7.1 Software Functions and Implementation

Figure 6.7-1 describes the software system functions to control engine speed, and the system level fail-safe features for defenses against unintended engine power. This simplified block diagram was developed from source code inspections, schematic inspections, interviews with TMC engineers, and TMC documentation.

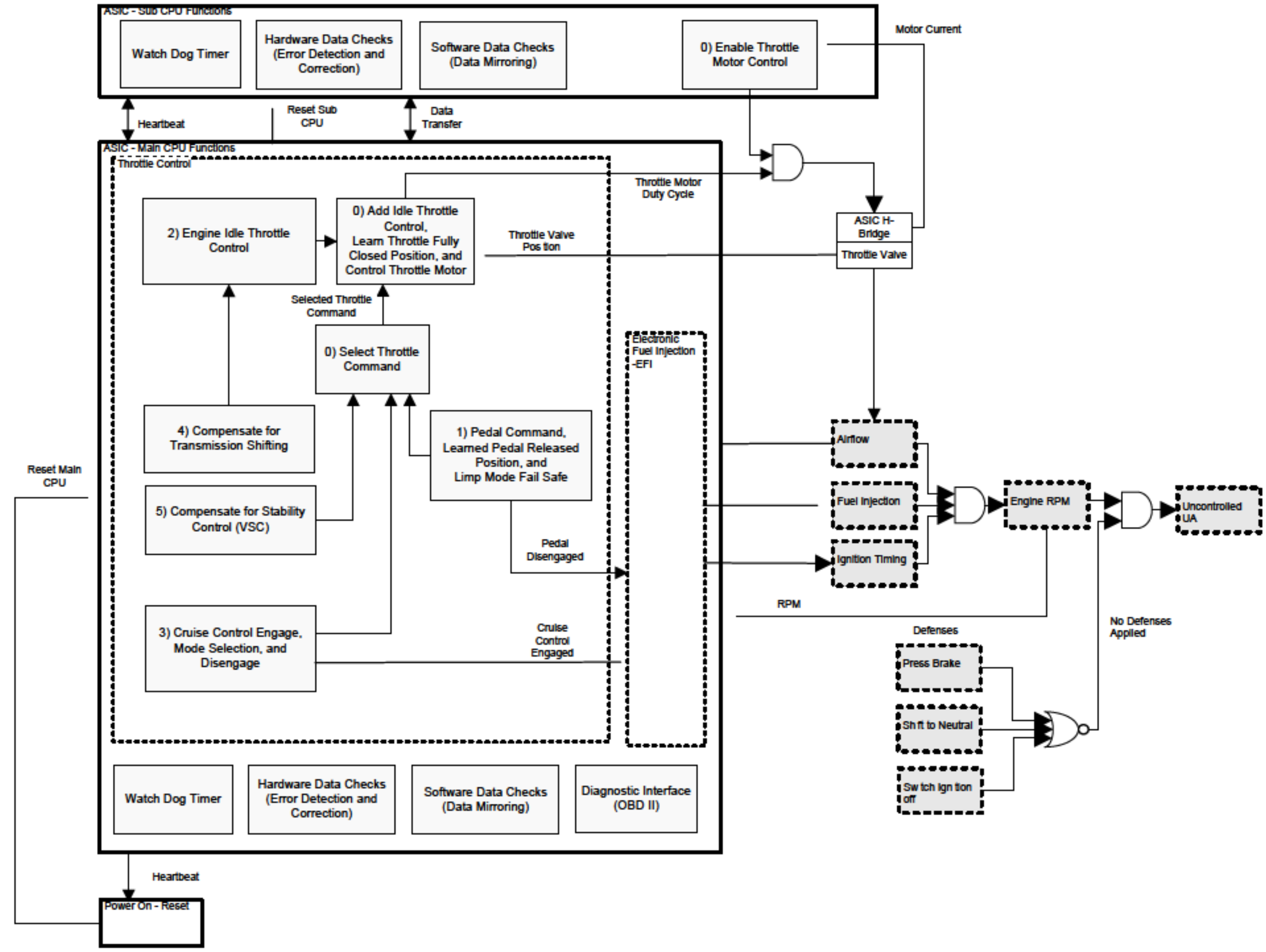

ASIC - Sub CPU Functions
Watch Dog Timer
Hardware Data Checks (Error Detection and Correction)
Software Data Checks (Data Mirroring)
0) Enable Throttle Motor Control
Motor Current
Heartbeat
Reset Sub CPU
Data Transfer
ASIC - Main CPU Functions
Throttle Control
Throttle Motor Duty Cycle
2) Engine Idle Throttle Control
0) Add Idle Throttle Control, Learn Throttle Fully Closed Position, and Control Throttle Motor
Throttle Valve Pos tion
ASIC H-Bridge
Throttle Valve
Selected Throttle Command
0) Select Throttle Command
Electronic Fuel Injection -EFI
4) Compensate for Transmission Shifting
1) Pedal Command, Learned Pedal Released Position, and Limp Mode Fail Safe
Airflow
Reset Main CPU
5) Compensate for Stability Control (VSC)
Fuel Injection
Engine RPM
Uncontrolled UA
Pedal Disengaged
Ignition Timing
RPM
3) Cruise Control Engage, Mode Selection, and Disengage
Cruise Control Engaged
Defenses
No Defenses Applied
Press Brake
Sh ft to Neutral
Sw tch Ign tion off
Watch Dog Timer
Hardware Data Checks (Error Detection and Correction)
Software Data Checks (Data Mirroring)
Diagnostic Interface (OBD II)
Heartbeat
Power On - Reset

Figure 6.7-1. Software Functions and System Safety

The desired engine speed and power determines the throttle position, the fuel injection quantity, and ignition timing. To increase engine speed to the maximum limit requires the correct and precise control of airflow, ignition timing, and fuel injection. Opening the throttle is necessary, but not sufficient to cause this maximum increase in engine speed.

The following sections describe software functions and system fail-safe features with a focus on the controls and barriers in place to control engine speed.

6.7.1.1 Main CPU Functions

The Main CPU primary functions are analog and digital sensor input, control output, and functional processing of the throttle valve, fuel injectors, and ignition timing. The Main CPU also provides an independent PWM control for the H-Bridge motor drive of the throttle valve. The majority of the processing occurs within the Main CPU.

6.7.1.1.1 Pedal Command

The Pedal Command function determines the driver commanded vehicle acceleration from two pedal sensor inputs. The two sensors provide pedal command input and pedal diagnostic capabilities. A valid relationship between the two sensor values must exist for the vehicle to operate normally.

The pedal command is sensed by the software as the difference between the pedal released position and the pedal pressed position. The pedal released position sensor values are learned values stored in SRAM. Under specific conditions, a software function adjusts these released position values when the pedal is not pressed. The general conditions are described below.

To learn a lower value:

- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

When one pedal sensor is determined to have failed, a "Limp Mode Fail Safe" is entered. In this mode, the failure is annunciated, and the acceleration commanded from the pedal is constrained. This allows the driver to control the vehicle at a limited engine speed.

If diagnostics detect a second pedal failure while in this "Limp Mode Fail Safe", the engine idles.

6.7.1.1.2 Cruise Control

The cruise control function automates the vehicle commanded acceleration to maintain a set speed. The cruise control modes are Cancel, Main, Resume, and Set. When enabled, the cruise control driver commands are as follows:

Table 6.7.1-1. Cruise Control States

Cruise Control State	Activation	Description
Coast	Set switch is engaged for longer than 0.6 seconds	While engaged, coast will decrease the speed of the vehicle at a rate of 0.06 g (or 2.12 kph/s). When disengaged the new vehicle speed becomes the set speed.
Tap Down	Set switch is engaged	Each time the set switch is engaged the vehicle speed will decrease by 1.6 kph and becomes the new set speed.
Accel	Resume switch is engaged for longer than 0.6 seconds	While engaged, accel will increase the speed of the vehicle at a rate of 0.06 g (or 2.12 kph/s). When disengaged the new vehicle speed becomes the set speed.
Tap Up	Resume switch is engaged	Each time the resume switch is engaged the vehicle speed increases by 1.6 kph and becomes the new set speed.

The cruise control states are commanded through one analog input. The single voltage determines the position of the cruise control input switch. Hardware failures of this switch were presented in Section 6.6.4.

The cruise control operation may be cancelled by software diagnostics that indicate an anomaly with the brake switch, vehicle speed sensing, and software data mirror failures.

The cruise control operation may be manually canceled through four different driver actions:

1. Cancel switch is engaged
2. Main switch is turned off
3. Brake is depressed
4. Shift from drive

Cancelling cruise control tests were also presented in Section 6.6.4.

6.7.1.1.3 Compensate for VSC

VSC primary function is to keep the vehicle in a correct attitude or orientation on the road. The stability control will cause the vehicle to brake and decrease the throttle angle if the actual vehicle yaw rate varies from the commanded vehicle yaw rate. The commanded yaw rate is based on the steering wheel and the vehicle yaw rate is sensed from 2 MEMS gyros. Braking request from the stability control will also cancel cruise control, if it is active.

Traction Control's (TRAC) exists within the VSC software. The TRAC primary function is to keep the difference between the drive wheels' speed and the vehicle speed minimal. In MY 2005 Camry vehicles, the TRAC function only decreases throttle.

VSC calculates the vehicle speed, which is used by TRAC, from 4 wheel sensors, one sensor per wheel. If a speed sensor fails, then the VSC function will stop (DTCs C0200, C0205, C0210, and C0215). The drive wheel speed is averaged between the values of the two front wheel speeds.

6.7.1.1.4 Transmission Shifting

Transmission shifting contribution to the control of the throttle valve is applied through the ISC.

6.7.1.1.5 Add Idle Engine Speed

In order to keep the engine speed above a stall condition, engine ISC commands the engine speed based on engine loads, including transmission shifting, and engine temperature. Engine temperature determines the unloaded idle speed. Additional loads, such as headlights or air conditioning loads, require an increase in the engine speed. These increases are summed with the unloaded idle speed. This summed engine idle contribution is added to the one selected throttle command to determine throttle valve position. Only one of the throttle command inputs is selected as the basis for positioning the throttle valve. The driver pedal, cruise control, and stability control are mutually exclusive.

It should be noted that the common notion of an idle engine occurring only when the vehicle is stopped and the driver's foot is off the pedal does not apply here. Engine idle speed contributes to the total throttle command whenever the engine is running.

6.7.1.1.6 Control Throttle Motor

The total throttle command is converted to the required pulse width (PWM duty cycle) to drive the throttle motor against its return springs. When driven, the throttle motor rotates the throttle valve. The throttle valve position is sensed by two sensors. A valid relationship must exist between the two sensor values for the vehicle to operate normally. The position sensors provide closed-loop feedback to the throttle motor driver. The throttle motor driver adjusts the pulse width to drive the throttle motor until the sensed position matches the commanded position.

To control the throttle valve position, the throttle valve fully-closed position is learned. This learned value is adjusted a maximum of [redacted] degree at each engine startup, when the throttle is closed under spring tension, and the throttle motor is not powered. The commanded throttle position is relative to this learned fully-closed position value. The general conditions for learning the throttle valve fully-closed position are as follows:

- [redacted]
- [redacted]
- [redacted]

The ASIC H-Bridge provides the power and pulses to drive the throttle motor. The H-Bridge requires inputs from both the Main and Sub CPUs to operate, and it is able to power the throttle motor only when both CPUs outputs are available. During any CPU reset, the CPU outputs to the H-Bridge that drive the throttle motor are pulled-low, disabling the motor drive.

Motor current is an indicator of how hard the throttle motor is being driven. If the throttle valve does not mechanically move, the motor will be driven hard to try to meet the commanded position. When the motor drive current crosses the over-current threshold, the sub CPU removes its input to the ASIC H-Bridge and this disables the motor drive.

If a throttle valve position sensor fails, power is cut to the throttle motor.

6.7.1.2 Sub-CPU Functions

The Sub CPU primary functions are analog and digital sensor input, control output, passing inputs to the Main CPU, diagnostics for the brake switch, and diagnostics for the cruise control main switch. The Sub-CPU also provides an independent hardware enable for the H-Bridge motor drive of the throttle valve. It does not implement a dual processing path in parallel with the Main CPU functions.

6.7.1.3 ECM Software Implementation

The ECM (engine control module) for the MY 2005 Camry uses a NEC V850 E1 processor. The software for the ECM is written in ISO/ANSI C[21], and compiled for production use with the GreenHills[22] compiler suite version 3.4.0. The code relies on the use of the Greenhills compiler with pragma directives[23] that is discussed below. Some basic statics on the source code are summarized in Table 6.7.4-1.

Table 6.7.4-1. Basic Code Size Metrics Camry05 Software

C code	#Files	SLOC	NCSL	Comments	NCSL/File	SLOC/NCSL	Comments/NCSL
sources	1,761	463,473	256,647	241,683	145.7	1.8	0.9
headers	1,067	100,423	39,564	67,064	37.1	2.5	1.6

The ECM is designed to meet a range of real-time constraints for engine control. The real-time operating system used is based on the OSEK[24] standard for distributed control units in vehicles, which is supported by AUTOSAR[25] (Automotive Open System Architecture) of which TMC is a core member. The operating system is based on the execution of tasks, each with a fixed and

[21] http://en.wikipedia.org/wiki/ANSI_C
[22] http://www.ghs.com/
[23] http://gcc.gnu.org/onlinedocs/cpp/Pragmas.html
[24] http://en.wikipedia.org/wiki/OSEK, http://portal.osek-vdx.org/files/pdf/specs/os223.pdf
[25] http://en.wikipedia.org/wiki/AUTOSAR

statically assigned priority. The MY 2005 Camry code contains [redacted] Tasks that execute at fixed priority levels between 1 [redacted].

The execution of a task can be interrupted, for short durations of time, by hardware interrupts, e.g., to signal the arrival of inputs or network data. A total of [redacted] interrupt levels are defined. [redacted] are dedicated to hardware traps (e.g., for attempts to execute illegal instructions or to access non-existing memory locations.

The priority levels are statically assigned and do not change dynamically.

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

6.7.2 System Integrity and Fail Safe Modes

6.7.2.1 Power On – Reset

The Power On – Reset function in the power supply ASIC contains voltage threshold monitoring based on sufficient supply voltages. Both CPUs are held in a reset state until the proper voltages are available. A heartbeat error between CPUs or low supply voltage can trigger the power supply ASIC to reset both CPUs. Both CPUs remain reset until the supply voltage and the heartbeat is restored.

During power on reset, the CPU outputs to the H-Bridge that drive the throttle motor are pulled-low, disabling the motor drive.

6.7.2.2 Heartbeat

The heartbeat pulse train signal from the Main CPU is provided to the power ASIC and also to the Sub-CPU. The Sub-CPU watchdog pulse train is provided to the Main CPU. The Main CPU can reset the Sub-CPU and the power ASIC can reset the Main CPU and Sub-CPU. The heartbeat pulse train is software generated and acts as an external indication of proper CPU hardware and software operation.

During any CPU reset, the CPU outputs to the H-Bridge that drive the throttle motor are pulled-low, disabling the motor drive.

6.7.2.3 Watch Dog Timer

Implemented in hardware, one watchdog timer exists in the sub CPU, and one exists in the Main CPU. Each watchdog timer is initiated at startup, and requires constant re-initiation by software. If a watchdog timer expires without being re-initiated by software, the CPU hardware is reset and restarts. The software function that re-initiates the watchdog timer executes in the lowest priority task. If this lowest priority task does not execute, it indicates abnormal processing or timing within either the software or hardware.

During watch dog timer reset, the CPU outputs to the H-Bridge that drive the throttle motor are pulled-low, disabling the motor drive.

6.7.2.4 Hardware Data Checks

Implemented in hardware, error detection and correction (EDAC) logic can detect and correct a hardware error in a memory location for single bit errors. This detection and correction occurs without affecting the software execution. If a hardware error occurs in a memory location altering two bits, it can be detected, but not corrected. EDAC is intended to detect and correct hardware errors in memory locations, and does not detect or correct software errors.

6.7.2.5 Data Transfer

Data is transferred between the two CPUs on a synchronous serial data bus. The serial data transfer implements no data checks and implements no retry capability. The data is transferred and refreshed every 8 ms.

6.7.2.6 Software Data Checks

A subset of software data is protected by implementing software data mirroring. When the data is written, a second location is written with the complement of the data. When the data is read, the second location is also read and checked. If the check fails, a default value is used.

When this software data mirroring is used, it protects data from being overwritten, such as by stack or buffer overflows.

6.7.2.7 Fuel Cut and Electronic Fuel Injection (EFI) and Ignition

When the pedal position sensors indicate the driver foot is off the pedal, a fuel cut function is used to limit maximum engine speed. An exception is when cruise control is engaged. When cruise control is engaged, this fuel cut function is disabled.

The moment the pedal is disengaged, the engine speed is sensed, and this level determines whether fuel cut is enabled. Fuel cut is enabled when this engine speed is above the fuel cut threshold. Following fuel removal from the engine, the speed decreases. When the engine speed reduces below the fuel cut recovery threshold, fuel is restored to the engine.

EFI controls the ignition timing based upon crank shaft timing, and controls the fuel and airflow mixture based upon the airflow through the throttle valve.

6.7.2.8 Onboard Diagnostic Interface (OBD II)

An onboard diagnostic serial interface allows technicians to analyze specific data values sampled from the ETCS-i. It also has the capability to modify values and the behavior of the system. The interface is enabled when connected to external diagnostic equipment.

6.7.3 Software Study and Results

The software study applied analysis and modeling tools to the actual MY 2005 Camry source code. Models were developed of functional areas to achieve an integrated understanding of the system behavior and simulations were run on these models to explore areas of interest. These simulations were confirmed against vehicle hardware, and the models were further refined. Ultimately, the software study supported the development of specific vehicle hardware tests.

Major CPU and software failures are protected through Sub-CPU and Main CPU checks, watchdog, heartbeat, and voltage monitoring. Data corruption is protected through EDAC and software-implemented data mirroring. Data limits are applied to detect sensor and output failures.

Described in the previous sections, specific tests were selected and tested on Camry vehicles. Many of these tests were the result of software code paths and variables that were identified as influencing the throttle valve position. During the software study, code paths and variables that possessed ALL of the following attributes were identified as candidates for testing on the Camry vehicles.

1. The candidate code path or variable data would require a mechanism to create sensor or data errors. External sensor or external control failures were tested extensively. Internal software data corruption could not be demonstrated.
2. The sensor or data error would need to persist to match reported UA behaviors. Most sensor and control data in the system is updated every compute cycle (at most every 16 msec); however, for the UA to persist, the sensor or data error would need to persist and would not be corrected or updated.
3. The sensor or data error would need to have an influence upon opening the throttle position, and possibly, increasing fuel flow and ignition timing.
4. The sensor or data error would need to occur without producing any error code or initiating the entry into any fail-safe mode.

The following section provides a brief introduction to the context of the study into possible software causes for UA in TMC vehicles. Detailed description of the software analysis is provided in Appendix A.

6.7.3.1 Software Analysis Scope and Technologies Applied

The study focused on the MY 2005 Camry L4 (inline four cylinder engine) ECM software.

The study started mid April 2010 and ran through mid August 2010. Initially, the software study was supported by the TMC facility in Torrance, California. The effort expanded to two facilities; one in Torrance and one in San Jose, California. This second facility became operational in June 2010.

Software tools provided by TMC included the Atlas translation software system for rough online translations from Japanese into English, and a version of the compiler suite that TMC uses to compile their source code. The proximity of the work area to TMC Headquarters facilitated a direct interaction between the NESC software team and the TMC engineers. The discussions took place in English and Japanese, with the help of an interpreter who provided two-way translations during all regularly scheduled and impromptu meetings and discussions.

The software team performed an analysis of the MY 2005 Camry L4 ECM software to investigate if there can be plausible triggers for UA in the TMC engine control software. As part of this study, the NESC team also analyzed the overall structure and of this software.

The fishbone diagram in Appendix B provides the general context for this study. The fishbone diagram groups potential software causes in four broad categories. In this report, the team addressed each of these categories:

1. Coding defects (implementation)

   Implementation in software, just as in hardware, can introduce defects when translating from design to code. To some extent, the software language used determines the types of defects that can be introduced. Coding standards can reduce the introduction of these defects by constraining the implementation techniques used and enhancing code inspections. For this study, tools were used to automate the code inspections by analyzing the source code and evaluating it against coding standards.

2. Algorithm flaws (design logic)

   The design and logic of a system can be analyzed to determine if the system functions as intended. Models of the functional system were developed, and these models facilitated the communication of the system behavior to the entire team. Analysis of these models, both manual and automated, produced areas of interest and prioritized the study efforts.

3. Task interference (race conditions, data corruption)

The design and implementation of the timing and order of the tasks within the system involves scheduling and control of task dependencies. Task dependencies can be execution order, data update and data usage sequencing, synchronous execution to an event, and asynchronous execution to an event. When control is not designed or implemented correctly, race conditions occur or data corruption occurs.

4. Insufficient fault protection

   Fault protection is required in any hardware and software system. Hardware failures and unexpected software states need to be recognized and mitigated.

6.7.3.2 Software Implementation Analysis Using Static Source Code Tools

The initial focus in analyzing the Camry MY 2005 source code has been on a thorough static source code analysis of the ECM source code to find possible coding defects and potential vulnerabilities in the code.

Tools Used:

- Coverity[26] – is currently one of the leading static source code analysis tools on the market. It excels at finding common coding defects and suspicious coding patterns in large code bases, taking a relatively short amount of time. The tool also supports custom-written checkers that can verify compliance with user-defined additional coding rules. This capability is put to use by using a small set of such Extend checkers. Coverity aims to reduce the number of warnings it issues to a minimum, by a careful filtering process that seeks to identify the most relevant or critical issues.

- CodeSonar[27] – is a second strong static source code analysis tool from Grammatech that uses a different technology for detailed inter-procedural source code analysis. CodeSonar analysis typically takes longer to complete than comparable tools, but can reveal more subtle types of defects and suspect coding patterns, requiring deeper path analysis (which can be more time consuming). The version of CodeSonar used was extended with checkers for JPL's coding standard. In this study, separate results for the coding standard checks from the default results were used.

- Uno[28] - is a research tool for performing static source code analysis, originating at Bell Labs. It is designed to perform a simpler, fast analysis for intercepting primarily the three most common types of software defects in programs: the use of uninitialized variables, **N**il-pointer dereferences, and out-of-bounds array indexing. The tool can be extended with user-defined checks.

[26] http://coverity.com/
[27] http://grammatech.com/products/codesonar/overview.html
[28] http://spinroot.com/uno/

6.7.3.3 Software Logic Model Checking Using the SPIN Tool

Another technology used was that of logic model checking. The leading tool in this domain is the Spin verifier, which was developed by one of the authors of this report.

Tools Used:

- Spin[29] - is an open-source software tool for the formal verification of distributed software systems. It is used frequently for the verification of mission or safety critical system designs. The tool was originally developed at Bell Laboratories in the Computing Sciences Research Center, and has been available since 1991. In April 2002 the tool was awarded the ACM System Software Award for 2001. It is possible to use this tool both for the exhaustive verification of high level design models of a system and for the detailed exploration of implementation level code in multi-tasking or multi-threaded systems.
- Swarm[30] – is a preprocessing system for Spin that can maximize use of available compute resources in large compute clouds or grids. It can also be used to make optimal use of all the CPU cores on a single compute server, to allow for a comprehensive analysis of large and complex software systems with a swarm of small verification jobs that jointly span the search space.

6.7.3.4 Software Algorithm Design Analysis Using MATLAB Models

Model-Based Design (MBD) is a mathematical and visual method of addressing problems associated with designing complex control systems. It is used in many motion-control systems, industrial equipment, aerospace, and automotive applications.

MBD provides an efficient approach for establishing a common framework for communication throughout the design process while supporting the development cycle ("V" diagram). In MBD, development is manifested in the following steps: modeling a system, analyzing and synthesizing a controller for the system, simulating the system, and integrating all these phases by implementing the system.

This study of the MY 2005 Camry software, model-based design techniques were applied to create high-fidelity models of the software functions and behaviors. TMC documentation and discussions with their engineering experts initiated the process. Source code analysis continued the process by increasing the accuracy of the models. And testing upon the Camry simulators and actual Camry vehicles confirmed the accuracy of the models. Efforts were made to incorporate as much actual source code into the models for further increased fidelity of the models.

[29] http://spinroot.com/spin/

[30] http://spinroot.com/swarm/

This MBD approach also supported the dissemination of the software functions and behaviors to the team as a whole. Presentations of the software in this manner efficiently communicated the software within the MY 2005 Camry microcontrollers without exposing the native source code.

Tools used are as follows:

- MATLAB – is a product family providing a high-level programming language, an interactive technical computing environment, and functions for algorithm development, data analysis and visualization, and numeric computation.
- Simulink - is an environment for multi-domain simulation and MBD for dynamic and embedded systems. It provides an interactive graphical environment and a customizable set of block libraries that let you design, simulate, implement, and test systems.
- Stateflow - extends Simulink with a design environment for developing state charts and flow diagrams. Stateflow software provides the language elements required to describe complex logic in a natural, readable, and understandable form. It is tightly integrated with MATLAB and Simulink products, providing an efficient environment for designing embedded systems that contain control, supervisory, and mode logic. Models can be created of embedded software that combine logical behavior, such as fault management and mode switching, with algorithmic behavior, such as feedback control and signal conditioning.
- SystemTest – automated model testing of Simulink models as a “black box”. Test values are provided to the proper model inputs; outputs of the model are tested against properties to obtain fail/pass results.
- aiT from AbsInt - statically computes tight bounds for the worst-case execution time (WCET) of tasks in real-time systems. aiT directly analyzes binary executables and takes the intrinsic processor cache and pipeline behavior into account.

6.7.3.5 Software Analysis Results

O-6. *While not resulting in a design vulnerability, the MY 2005 Camry source code required unique code inspection tools, and manual inspections due to:*

a. The TMC software development process uses a proprietary developed coding standard.

b. Industry standard static analysis tools provide automated code inspections based upon industry standard code implementations.

O-7. *There are no methods for capturing pre-event software state and performance following an UA event either on the vehicle or as a diagnostic tool.*

F-10. *Extensive software testing and analysis was performed on TMC 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 UA were not found.*

6.8 Vehicle EMC Testing in Support of the Study of Unintended Acceleration in Toyota Vehicles

Electromagnetic Interference (EMI) can affect electronics in unexpected ways and may not leave physical evidence to guide troubling shooting of unwanted effects. Because of this non-degrading momentary condition, EMI is often postulated as a cause for the UAs described in the VOQ data.

The NESC team tested six VOQ vehicles to test levels significantly above European certification levels and natural environments without observing any opening of the throttle. EMI testing found no evidence of hardware or electro-magnetic interference (EMI) induced vulnerabilities in a consumers use of the vehicle that would open the throttle in a manner that can explain the VOQs.

Comprehensive EMC testing, including radiated susceptibility, conducted transient emissions and conducted transient, audio and RF susceptibility, described in the 3 sections that follow, was performed in support of the investigative process. Six Toyota Camry vehicles listed in Table 6.8-1, all identified as VOQ vehicles, were provided by the NHTSA and were all tested in this effort. The purpose of the testing was to identify, if possible, any vulnerabilities in the design that could lead to or result in an unintended or uncommanded acceleration in the presence of interfering signals emanating from outside or inside the vehicle. Directly because of this reason, the levels of exposure utilized in this effort were well above those normally employed for certification in the automotive industry. Figure 6.8.1-1 compares typical certification levels of about 30V/m, Toyota test levels of 60 V/m, Toyota Internal Test Levels of 100V/m and the NESC test levels of 100 to 250V/m. The facility used for the testing activities was selected on the basis of several criteria, including staff knowledge and expertise, flexibility in scheduling, accommodation of non-standard testing, availability of vehicle dynamometers for the radiated immunity testing and, perhaps most important, the presence of a reverberation chamber to facilitate rapid external RF exposure of the vehicles over a wide portion of frequencies in the most efficient manner.

Summary Conclusion

Vehicles were placed in operational modes in gear on a dynamometer to simulate driving conditions. All of the vehicles performed very well under radiated and conducted immunity testing. In some cases vehicles reacted to a RF environment significantly above certification requirements. Reactions ranged from the setting of DTCs, dashboard lights changing state, engine speed reducing, or the engine stalling. These vehicle effects indicate that some susceptibilities are present at RF levels far in excess of certification levels. No occurrences of unintended or uncommanded acceleration were observed. Some effects were noted at signal levels and coupling methods not expected in normal operating environment.

During the course of the EMI testing to identify the threshold of susceptibility, one effect was observed that opened the throttle when subjected to conducted EMI levels far in excess of any signal sources and coupling method present in a vehicle. An increased engine speed response to the presence of a large conducted audio frequency signal, injected in differential mode, simultaneously onto both accelerator pedal sensor signal lines using capacitive coupling was noted. The large magnitude of this signal was injected only onto the two wires pulled out of a six-wire harness bundle and thus isolated and was injected the noise in a fashion that would not be encountered during consumers' use of the vehicle. Testing per this unique test scenario resulted in no DTCs being set or in any UA prior to application or subsequent to removal of the stimulus.[31] The NESC team did not look at possible implications of aftermarket non-OEM additions such as remote start or cruise control systems.

Table 6.8.1-1 below summarizes the test levels and how each of the six VOQ vehicles responded to the test levels.

General Test Aspects

All aspects of testing were guided by test plans and procedures. Safety measures were determined and employed throughout testing, including use of adequate vehicle tie-downs, vehicle cooling ventilation, and vehicle exhaust ventilation. Each vehicle was checked for fault codes before and after each task and at appropriate times during the performance of each task. Unless otherwise specified in a particular test segment, general vehicle conditions for all testing utilized windows on the vehicle in the fully open position, doors closed, engine at operating temperature, and unless otherwise defined, all switchable features/accessories turned off. Upon arrival at the test facility and after all immunity exposures, each vehicle was checked to verify normal function of the vehicle engine control system, speed control, and vehicle driving handling. A Toyota Techstream was connected to the OBD II interface to verify proper signal levels for accelerator and throttle sensing and control signals.

VOQ Vehicles

Six VOQ vehicles were subjected to detailed EMI testing. The vehicle models along with a summarized description of the VOQs are listed in the Table 6.8-1.

[31] Two pedals failed due to high currents reference failure analysis report# NHTSA-NVS-ETC-SR15.

Table 6.8-1. VOQ Summary Description

Veh ID.	MY	VOQ#: Summary description
13C	2002, Camry XLE V6	10319308: The vehicle was idling in neutral or park; the driver put his/her foot on the brake and shifted into drive; virtually simultaneously the engine accelerated rapidly. In each case the driver's foot on the brake prevented the vehicle from moving forward with any speed, but it was necessary to press hard on the brake -- and even with that in at least one instance the vehicle strained and bucked. The situations were resolved when the driver shifted to neutral or park.
15C	2003, Camry XLE L4	10283433: One week after the purchase I was at a stop sign, with my foot on the brake, and the vehicle suddenly accelerated. I tapped the accelerator, but the engine continued to accelerate with the tachometer reading nearly 9,000 rpm's. I turned the engine off with the ignition.
14C	2004, Camry XLE V6	10321093: Driving approximately 5 mph attempting to stop, the brake pedal was engaged with an unexpected acceleration. The vehicle was able to stop with extreme pressure applied to the brake. The identical failure occurred on ten separate occasions.
18C	2004, Camry L4	10327490: Reversing at 5mph into a parking space there was sudden acceleration into an apartment building. The vehicle was then put in park and turned off.
12C	2007, Camry XLE V6	10319201: As I removed foot from brake to gas pedal to pull into garage, and lightly placed foot on accelerator, instantaneously engine revved, pedal went to floor, tach zoomed and auto jetted into garage. I immediately hit brakes with both feet, attempting to disengage transmission from D and put into N. Gear shift erratically plunged into R and vehicle began to go backwards with engine throttle wide open. Again, I tried to jam gearshift to N or P, and vehicle jettisoned forward hitting garage wall at full force. – again tried to force it into P, and it again went to R, then again forward in another direct hit against garage wall, breaking the wall open and splitting sheetrock as auto nearly popped through to laundry room and gas furnace. I held the push-button in while simultaneously forcing gear shift again to reach P. Engine went from full-bore open to a stop.
19C	2007, Camry L4	10326416: Waiting at a red light when the vehicle revved and lurched forward and hit the vehicle in front of me, bounced off and hit it again. I pressed the brakes as hard as I could, but it took a few moments before the vehicle would stop. This vehicle was in just the week before for the recall fix for the accelerator pedal.

6.8.1 Radiated Susceptibility Testing

Radiated susceptibility testing subjected the vehicles under test to RF fields in excess of certification and Toyota acceptance levels. The NESC test levels shown in blue in Figure 6.8.1-1 are higher levels than Toyota test levels shown in red and the European certification levels shown in green.

NESC test levels were chosen at 100 V/m to establish a higher than normal threat baseline, with steps to higher levels in threat bands occupied by common emitters potentially encountered during vehicle operation. The steps to higher levels of 150V/m and 200V/m correspond to levels with margin to theoretical threat level scenarios higher than expected from amateur and commercial band transmitting.

The RF Electromagnetic Susceptibility Test was performed in four parts with results summarized in columns a) through c) of Table 6.8.1-1.

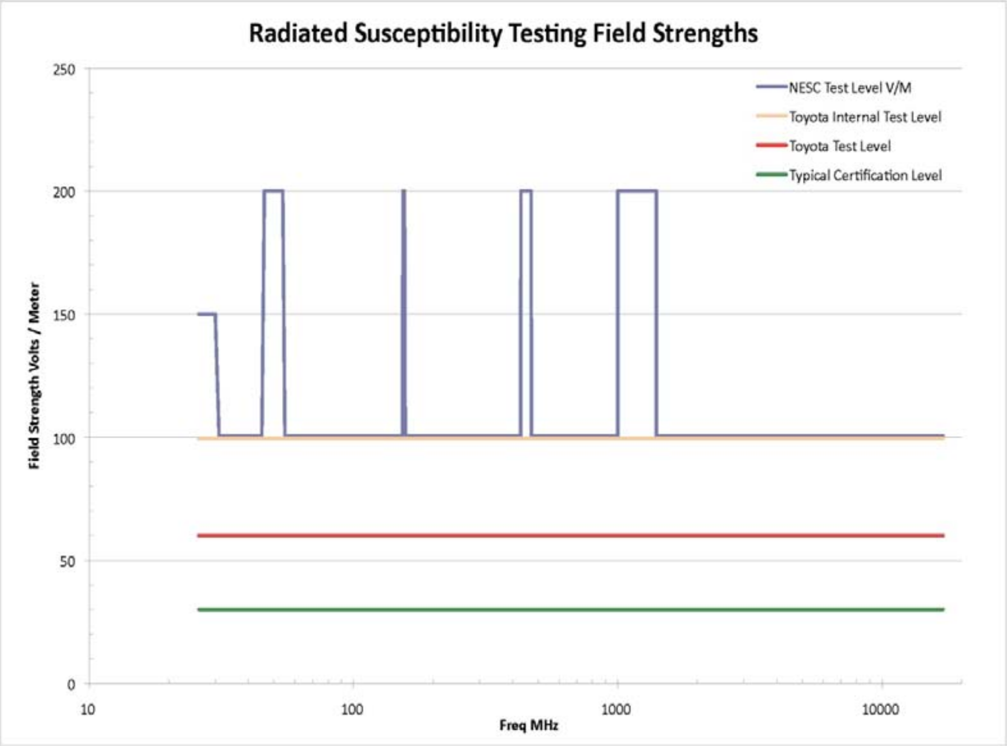


Figure 6.8.1-1. Radiated Susceptibility Test Field Strengths

6.8.1.1 Radiated Electromagnetic Susceptibility Test

The RF Electromagnetic Susceptibility Test applied externally to the vehicle was performed in 3 parts with results summarized in columns a) through c) of Table 6.8.1-1.

Purpose: Expose the vehicles to RF fields to determine if any susceptible conditions are evident.

Reference test method: ISO 11451-2

Vehicle preparation: Vehicles as close to production condition as possible. DTCs were read and recorded prior to and following testing.

Vehicle Test Condition: Vehicles were operated on a 4-wheel dynamometer under steady state conditions. Vehicle accelerators were affixed in degree of application using a mechanical positioning device.

Vehicle orientation: For the vehicle transverse electromagnetic (TEM; vertical polarization only) chamber, and the reverberation chamber (homogenous field polarizations), one vehicle position was utilized. For the semi-anechoic chamber, 8 vehicle orientations at 45 degree increments with horizontal and vertical polarization test signal exposures were utilized.

Test set-up: For the TEM and reverb testing, the vehicles were essentially immersed in the radiated electric fields. For the semi-anechoic chamber testing, the vehicle to antenna separation was such that the entire vehicle was illuminated within +/-3 dB.

RF Test Signal levels:

26 MHz to 3.2 GHz except for bands below	100 V/m
26 – 30 MHz, 46 – 54 MHz,144 – 160 MHz 430 – 470 MHz,5.2 – 6.0 GHz,9.0 – 9.5 GHz,15.7 – 17.7 GHz	200 V/m
1.0 GHz - 1.3 GHz, 2.7 – 3.2 GHz	200+ V/m

RF Test Signal Modulation:

26 MHz to 800 MHz	1 kHz 100 % modulation with 50% duty cycle
800 MHz to 3.2 GHz (except below)	Pulse Modulation per ISO 11451-1
1.0 – 1.4 GHz, 2.7 – 3.2 GHz, 5.2 – 6.0 GHz, 9.0 – 9.5 GHz, 15.7 – 17.7 GHz	3 usec @300 Hz rep rate

Frequency steps and duration The logarithmic step frequency method of ISO 11451-1 with 100 steps/decade was used. The dwell time was in accordance with ISO 11451-1 with 2 seconds minimum.

Data: Basic report data as defined in ISO 11451-2

Functions observed and documented included throttle position, changes in engine speed, changes in vehicle speed, unexpected transmission gear shifts, changes of gauges, indicator lights or lighting levels of the instrument cluster, audible noises, or other unexpected behaviors.

Methods of observation included audible noise events within the vehicle and/or test chamber (e.g., vehicle engine noise) via fiber optic microphone, instrument panel monitoring via fiber optic TV camera, and dynamometer control system monitoring.

Data associated with observed events included plots of the test signal exposure level and tabulations of anomalies observed, frequency and the threshold level for each anomaly. DTCs were read periodically and when events were observed and recorded via a Techstream.

6.8.1.2 Near Field Susceptibility Test

The RF Near Field Susceptibility Test and results are summarized in column d) of Table 6.8.1-1.

Purpose: Expose the vehicles to RF fields emanating from simulated hand held devices inside the vehicle passenger compartment to determine if any susceptible conditions are evident.

Reference test methods: ISO 11451-3 and ISO 11452-9

Vehicle preparation: Vehicles as close to production condition as possible. DTCs were read and recorded prior to and following testing.

Vehicle Test Condition: Vehicles were operated on a 4-wheel dynamometer under steady state conditions. Vehicle accelerators were affixed in degree of application using a mechanical positioning device.

Modules in the vehicle to receive near field exposure included: The engine controller, the transmission controller (where separate), the ABS Controller, the Throttle body assembly, the accelerator pedal assembly, and the cruise control switch assembly.

RF Test Frequency Bands and Power Levels:

26 – 30 MHz	10 Watts
46 – 54 MHz	10 Watts
144 - 160 MHz	10 Watts
430 – 470 MHz	10 Watts
800 – 900 MHz	5 Watts
1.8 – 1.9 GHz	2 Watts
2.4 – 2.5 GHz	1 Watt
5.7 – 5.9 GHz	2 Watts

Five frequencies were tested in each band including the band edges, the approximate center frequency, with the remaining two frequencies approximately evenly distributed in the band.

Antennas: The antennas used were low gain and were determined in discussions between the E3 team and the test lab to ascertain the most appropriate equipment to be used within the capabilities of the facility.

Data: Basic report data as defined in ISO 11451-3

Functions observed and documented included throttle position, changes in engine speed, changes in vehicle speed, unexpected transmission gear shifts, changes of gauges, indicator lights or lighting levels of the instrument cluster, audible noises, or other unexpected behaviors.

Methods of observation included audible noise events within the vehicle and/or test chamber (e.g., vehicle engine noise) via fiber optic microphone, instrument panel monitoring via fiber optic TV camera, and dynamometer control system monitoring.

Data associated with observed events included tables of the test signal frequencies, exposure levels and tabulations of anomalies observed, frequency and the threshold level for each anomaly. DTCs were read periodically and when events were observed and recorded.

6.8.1.3 Radiated Susceptibility Summary Results

Table 6.8.1-1 columns a) through d) summarize the four major tests and results. The observed effects at high RF levels include setting of DTCs, dashboard lights changing state, engine speed reduction, or the engine stalling. However no uncommanded throttle openings were observed.

Table 6.8.1-1. Test Environments, Levels and Vehicle Response Summary

			Radiated Susceptibility (6.8.1)				Conducted Emissions (6.8.2)	Conducted Susceptibility (6.8.3)									
Veh No.	MY	VOQ#	a) VTEM 26MHz – 30MHz (CB and Ham) 80% 1KHz AM Modulation 200 V/M, achieved 150 V/M	b) VATC 30MHz - 200MHz, 100 V/M with threat bands: 46-54 @ 200 V/M goal 156 – 154 @ 200V/M goal 200 – 800 MHz 100 V/M 430 – 470 MHz 200V/M 1KHz Square Wave Modulation	c) VRTC (Reverb) 800MHz 17.7GHz 1KHz Square Wave Modulation @ 100 V/M with threat bands: 1.0 GHz to 1.4 GHz @ 200V/M 2.7 @ 200V/M	d) Radiated Susceptibility - On-Board Transmitters 26MHZ-160MHz, 10-70W, 1kHz Modulation 430MHz-470Mhz, 10 W, CW 800MHZ-900MHz, 5W, cell phone modulation. 1.8GHz-1.9GHz, 2W, cell phone module. 2.4GHz-2.5GHz, 1W, 1.6kHz, 50% module. 5 antenna positions (maximum)	e) Transient Emissions – (per ISO 7637-2) Results in Table 6.8.2-1	f) Conducted Susceptibility – Power Line Transients (per ISO 7637-2 Test Pulses "1, 2a, 3a, 3b" per ISO 7637-2.	g) Conducted Susceptibility – Signal Line Transients (per ISO 7637-3, Test pulse "Fast A" "Fast B", "Slow +", "Slow –", per ISO 7637-3	h) Conducted Susceptibility – Extended Audio, Signal Lines, XFMR Coupled (adapted from ISO 11452-10, 2Vp-p, 15Hz-150kHz	i) Conducted Susceptibility – Extended Audio, (2Vp-p, 30 kHz-250 kHz) This test uses the same principles as column h, but Frequency range and coupling methods are different	j) Conducted Susceptibility – Extended Audio, Signal Lines 15 Hz- 250kHz (Reference ISO 11452-10, This test uses the same principles as ISO 11452-10, ,but with Variant specific signal lines and test frequencies.	k) Conducted Susceptibility – #1 Bulk Current Injection, (26MHz-400 MHz) (per ISO 11451-4) and special test 10 kHz to 10 MHz #2 The "special test" reference was the variant frequencies of column j on Denso pedal, using this coupling method	l) Conducted Susceptibility – Resistance loaded 5V regulator ECM 5V voltage line was loaded via a resistance box to drop voltage until a reaction was observed.	m) Power Quality – Voltage Variation (per ISO 16750-2 4VDC-18VDC on ECM power input lines.	n) Power Quality – Voltage Dips (per ISO 16750-2 Voltage applied to the supply voltage lines. A dip is from 11V to the dip voltage for the specified duration and then back to 11 V. The dip voltages are: 5.5 V, 5.0 V, 4.5 V, 4.0 V, 3.5V and 3.0 V. Dips to each voltage level are for 100 µs, 1 ms, 10 ms and 500 ms durations. The DUT operation shall be monitored during the dip test and the interval time between dips shall be sufficient to verify normal DUT operation. At each dip voltage, run through the range of dip durations.	o) Power Quality – Voltage Ripple (per ISO 16750-2) 1) 1.2Vp-p on ECM 12V power input lines 2) 0.5Vp-p on 5V ECM power line 3) 2Vp-p, 15Hz-250kHz on ECM 12V power lines. 4) 4Vp-p, 15Hz-250kHz on ECM 12V power lines.
13C	2002, Camry XLE V6	10319308	No Effects.	No UA Effects. NOTE: An ECM code of P1150 related to the A/F sensor was noted after test case.	No UA Effects. NOTE: 6-29-10 temp gage read high, not to boiling point, check engine light did not come on. Solution: redirect forced airflow into radiator.	No Effects.	No significant source/victim transient vulnerabilities were observed. Minor ignition noise on ECM +5v, Small coupling from door locks to +5v, VTA1 sensor, cam, air flow, brake signal	Test not performed on this vehicle									
15C	2003, Camry XLE L4	10283433	No Effects.	No Effects.	No Effects.	No Effects.	No significant source/victim transient vulnerabilities were observed. Minor ignition noise on ECM +5v, slight window actuator coupling to cruise control signal,	No Effects	No UA Effects. Cam sensor disrupted by slow transients, but not fast transients – caused engine stall.	No UA Effects. Mass Air Flow sensor affected by 15 Hz, 50 Hz, 100Hz and 200 Hz signals at 1.2V and engine continued running, but rough, up to 2.0V. Application at 2V caused engine to stall. At 600 Hz and above up to 10kHz no effect; at 10kHz instant stall of the engine. Cam sensor on 15C instant stall at 15, 500 Hz at 2 Vp-p. Threshold about 1.2Vp-p at 500 Hz. Crank sensor on 15C instant stall at 15 Hz @0.6Vp-p Throttle sensor on 15C 15 Hz @ 1Vp-p engine struggling; 1.2Vp-p slight speed-up and went into limp-home mode. Effects at other frequencies, but more immune at higher frequencies.	No UA Effects. Audio applied to the power lines resulted in only slight ripple on the 5V regulated voltage output.	Test not performed on this vehicle	1) There were no effects with the test signal applied to the ECM harnesses. There were no effects with the test signal applied to the Accelerator Pedal production configuration harness. 2) Test not performed, non Denso Pedal	No UA Effects Vehicle stalled when loaded with 5 ohms, regulated voltage dropped to 2.87 volts.	Test not performed on this vehicle	No UA Effects On 15C pin A1 stall at 10 ms and at 500 ms. Other power feeds no effect.	Test not performed on this vehicle
14C	2004, Camry XLE V6	10321093	No UA Effects. Note: Lights Came on the Instrument Cluster at CW, not during AM modulation ECM codes of P2239, P2241, and ABS code C1201 recur during testing.	No UA Effects. At 158 MHz, the vehicle engine shut down at 250 V/m DTCs reflected a cam sensor, and also included a crank sensor, and two ignition coil sensors. At 100 V/m speed decreased with the radiated field applied. The application of RF caused a decrease in speed only. Vehicle 14C ECM damaged during VATC testing. Engine ECM failed because of the unshielded OBD power connection.	No Effects.	No Effects.	Vehicle 14C unavailable due to ECM damaged during VATC testing.										
18C	2004, Camry L4	10327490	No Effects.	No UA Effects. NOTE: An ECM code of P1150 related to the A/F sensor was noted. The presence of this code is currently not deemed to be significant.	No Effects.	No Effects.	No significant source/victim transient vulnerabilities were observed. Minor ignition noise on ECM +5v, VPA1, VTA1, Small AC blower transients on VPA1, VTA1, Cruise, Crank, Cam, MAF, O2, Brake signals., Moderate door lock coupling to VPA1, VTA1, Cruise, O2, Brake signals. Spike from rad fan to O2 and brake input	No Effects	No UA Effects. Crank Sensor disrupted by slow transients, but not fast transients. Cam sensor disrupted by slow transients, but not fast transients – caused engine stall.	No Effects	No UA Effects. Audio applied to the power lines resulted in only slight ripple on the 5V regulated voltage output.	Test not performed on this vehicle	1) There were no effects with the test signal applied to the ECM harnesses. There were no effects with the test signal applied to the Accelerator Pedal production configuration harness. 2) Test not performed, non Denso Pedal	No UA Effects Vehicle stalled when loaded with 5 ohms, regulated voltage dropped to 2.87V.	No UA Effects with voltage varied (8 to 16 V) to ECM only; speedometer stopped functioning at 6V; engine ran rough at 5V; engine stalled @ 4V.	No UA Effects, but stalled engine at 3.5V @ 1ms on A1 line; 5.5V dips on B6 line on 18C caused brief engine speed increase as the ECM went into limp-home mode. In a modified test (Drop-outs - V dropped to 0) at 600 ms, the engine speed became unstable, but didn't stall. At 900 ms, the engine speed briefly increased to about 1500 rpm as the vehicle went into limp-home mode.	No Effects
12C	2007, Camry XLE V6	10319201	No Effects.	No UA Effects.	No Effects.	No Effects.	No significant source/victim transient vulnerabilities were observed. Small coupling from door locks to +5v, VTA1 sensor, cam, air flow, brake input, slight window actuator coupling to +5v	Test not performed on this vehicle				Inject both pedal sensors with differential mode signal Anomalies observed 200Hz 2Vpp 1500rpm 200Hz 1.8Vpp 1100rpm 200Hz 1.6Vpp 900rpm 200Hz 1.4Vpp 600rpm 200Hz 1.2Vpp 600rpm 300Hz 2Vpp 3000rpm 400Hz 2Vpp 4500rpm 400Hz 1Vpp 900rpm 400Hz 0.5Vpp 900rpm 500Hz 2Vpp 5000rpm 600Hz 1Vpp 1900rpm 700Hz 1Vpp 1700rpm 800Hz 1Vpp 1600rpm 900Hz 1Vpp 1600rpm 1kHz 2Vpp No Effect 10kHz 2Vpp No Effect 30kHz 2Vpp No Effect 50kHz 2Vpp No Effect 100kHz 2Vpp No Effect 150kHz 2Vpp 3300rpm 150kHz 1.8Vpp 1500rpm	1) There were no effects with the test signal applied to the ECM harnesses. There were no effects with the test signal applied to the Accelerator Pedal production configuration harness. 2) RPM increase when signals were applied to both pedal signal lines, both signal and voltage supply lines together, but at a broader frequency range around 100 kHz, but with no latch-up.	Test not performed on this vehicle	No UA Effects with voltage varied (8 to 16 V) to ECM only; speedometer stopped functioning at 6V; engine ran rough at 5V; engine stalled @ 4V.	Test not performed on this vehicle	No Effects
19C	2007, Camry L4	10326416	No Effects. Vehicle repeatedly exhibited loss of vehicle speed indication DTCs: Lo Rng. P0500 (Vehicle Speed Sensor), C0200 (Right Front Sensor), C0205 (Left Front Sensor), C0210 (Right Rear Sensor), C0215 (Left Rear Sensor), and C1237 (Speed Sensor Rotor Faulty)	No UA Effects.	No Effects.	No Effects.	No significant source/victim transient vulnerabilities were observed. Minor ignition noise on ECM +5v, Seat motor spike on brake signal, door lock on O2 and brake	Test not performed on this vehicle									

6.8.2 Transient Emission Testing

The conducted and coupled transient voltages were measured at the power leads and selected sensor leads of the ECM to see if any significant voltage pulses from potential transient generating sources were present. The list of potential transient generating sources was analyzed based on the nature of the load (inductive, resistive or capacitive), the current drawn by the load, and the technology used to switch the current to the load to determine those most likely to affect the ECM and are shown in Table 6.8.2-1. All of the measured transients at the ECM were small in magnitude compared to the test pulse levels applied to the ECM leads during that phase of the EMC testing. Results are summarized under the Conducted Emissions Column in the results Table 6.8.1-1 above. The ECM leads selected for transient emission measurements are listed in the Source Victim Coupling Matrix created by the NESC and shown in Table 6.8.2-1.

6.8.2.1 Conducted and Coupled Transient Analysis

Table 6.8.1-1 summarizes the Conducted and Coupled Transient Analysis test and results in column e.

Purpose: The purpose of this test was to measure the magnitude and time characteristics of electrical transients occurring in test vehicles while in various operational conditions.

Reference Test Method: SAE J1113-42 adapted to the measurement of electrical transients on a vehicle.

Vehicle preparation: Vehicles as close to production condition as possible. DTCs were read and recorded prior to and following testing.

Vehicle Test Condition: Vehicles were tested in static test bays, no wheels turning.

6.8.2.2 Conducted Transient Emissions Results

Results of CE testing are summarized in the Source Coupling Victim Table 6.8.2-1. No significant source/victim transient vulnerabilities were observed including no coupling from the brake switch to throttle control signal lines.

Some coupling was observed from the ignition noise to ECM +5V, VPA1, VTA1. Small coupling from door locks to +5V, VPA1, VTA1 Cruise control signal, cam sensor, air flow, O_2, brake input. Slight window actuator coupling to +5V, cruise control signal. Seat motor spike on the brake signal. Small AC blower transients on VPA1, VTA1, cruise, crank, Cam, MAF, O_2, brake signals. Spike from radiator fan to O_2 and brake input.
Coupled noise from the measured sources to the accelerator pedal and throttle sensor signals directly influencing the throttle measured less than (0.2V). The onboard coupling is much less than the levels conducted susceptibility testing imposed on these signals. There is a factor of at least a 10 margin between applied test levels and measured noise coupling.

Actuation of the brake pedal is often noted as the antecedent event for some UAs; therefore, emissions testing examined the effects of the brake switch on the system. Table 6.8.2-1 shows the testing on the brake switch for conducted transient emissions with no transient effects observed on victim circuits.

Conducted Susceptibility/Immunity testing of the brake switch signal line per columns g, h & j showed no UA effects. The line was also tested collectively in the wire harness via the Bulk Current Injection test in column k with no effects.

Table 6.8.2-1. Conducted Transient Emissions Source Victim Test Summary Matrix

Victim Circuit Source Component	ECM Power lead I	ECM Power lead V	Reg 5V	Accel Pedal VPA1 Sensor	Throttle Body VTA1 Sensor	Cruise Control Switch	Crank Sensor	Cam Sensor	Mass Air Flow Sensor	O2 Sensor	Brake signal Input
_Alternator / Ignition	NE, 3, 8, 14, 19	NE, 3, 8, 14 19	NE, 8, 14 19	NE, 2, 18	NE, 18	NE	NE	NE	NE	NE	NE
AC blower motor	NE	NE	NE	NE, 2, 15	NE, 15	NE, 15	NE, 15	NE, 15	NE, 15	NE, 15	NE, 15
Door lock Solenoids/motors	NE	NE	NE, 1	2, 4, 9, 16	1, 4, 9, 16	NE, 9, 16	NE	NE, 1	NE, 1, 18	NE, 4, 9, 16, 21	1, 4, 9, 16, 21
Driver seat motor fore/aft	NE	NE	NE	NE, 2	NE	NE	NE	NE	NE	NE	NE, 17
Driver seat motor up/down	NE	NE	NE	NE, 2	NE	NE	NE	NE	NE	NE, 6	NE, 6, 20
LF Window	NE	NE, 5	NE	NE, 2	NE	NE, 5, 10	NE	NE	NE	NE	NE
RF Window	NE	NE, 5	NE	NE, 2	NE	NE, 5, 10	NE	NE	NE	NE	NE
RF Window*	NE*	NE*	NE*	NE*	NE*	NE, 10	NE*	NE*	NE*	NE*	NE*
RR Window*	NE*	NE*	NE*	NE*	NE*	NE, 10	NE*	NE*	NE*	NE*	NE*
Windshield Wipers	NE	NE	NE	NE, 2	NE	NE	NE	NE	NE	NE	NE
Washer Pump motor	NE	NE	NE	NE, 2	NE	NE	NE	NE	NE	NE	NE
Hazard flashers	NE	NE	NE	NE, 2	NE	NE	NE	NE	NE	NE	NE
Brake switch load	NE	NE	NE	NE, 2	NE	NE	NE	NE	NE	NE	NE, 7, 11
Headlamps *	NE*	NE*	NE*	NE*	NE*	NE*, 10	NE*	NE*	NE*	NE*	NE*, 12
Horn	NE	NE	NE	NE, 2	NE	NE	NE	NE	NE	NE	NE
Heated Backlight	NE*	NE*	NE*	NE*	NE*	NE*	NE*	NE*	NE*	NE*	NE*, 13
Radiator & Cond fan motors	NE	NE	NE, 16	NE, 2	NE	NE, 17	NE	NE	NE	NE, 17	NE, 12, 17
Power Mirror Right	NE	NE	NE	NE, 2	NE	NE	NE	NE	NE	NE	NE
ABS Brake hydraulic motor *	NE	NE	NE	NE, 2	NE	NE	NE	NE	NE	NE	NE
ABS Pair solenoids *	NE	NE	NE	NE, 2	NE	NE	NE	NE	NE	NE	NE
Sun Roof *	NE	NE	NE	NE, 2	NE	NE	NE	NE	NE	NE	NE

NE = No Coupling Observed

12C: 1 = Small amount of coupling. 2= Reg 5V lead was measured rather than the Accel Pedal Sensor Lead

13C: 3 = Characteristic pulses from ignition system, 4 = Small amount of noise, 5 = 0.5 - 1.0V drop due to wire resistance, 6 = Transient Voltage Spike, 7 = 2V drop due to inrush current

15C: 8 = Characteristic transients from ignition pulses, 9 = Small amount of noise induced, 10 = Approx 0.5 - 1 Volt drop due to wiring resistance, 11 = Approx -2V transient on turn-off, 12 = Disturbance at turn-on, 13 = Approx -2V transient at turn-off

* Tested on 15C, 19C only

NE* = Vehicle 15C and 19C only tested

18C: 14 = Normal Ignition transient, 15 = Short Minor Coupling, 16 = Moderate Coupling, 17 = One significant spike, 18 = Very Slight Effect

19C: 19 = Characteristic Ign transients, 20 = One Significant 5V spike, 21 = Small amount of coupling, 22 = Moderate coupling

6.8.3 Conducted Susceptibility Testing

Conducted susceptibility testing includes an extensive battery of tests involving various frequency ranges, as well as transient pulses and waveforms, conducted onto signal and power lines. The following descriptions detail the tests performed. Columns f through o of Table 6.8.1-1 summarizes the battery of Conducted Susceptibility testing performed, and their results.

Purpose: The purpose of this task is to expose vehicle electrical systems to transient conditions that can be present in vehicle electrical systems.

Vehicle preparation: Vehicles as close to production condition as possible. DTCs were read and recorded prior to and following testing.

Vehicle Test Condition: Vehicles were operated on a 4-wheel dynamometer under steady state conditions. Vehicle accelerators were affixed in degree of application using a mechanical positioning device.

This phase of the testing consisted of several parts.

For all the tests, the engine was idling at operating temperature with the transmission in Park, unless otherwise noted. In all test methods, operation of the ECM was observed and any interactions recorded via a Techstream.

For the tests where the power leads to the ECM were tested, the battery leads to the ECM were severed from the vehicle harness and connected together, along with the ignition lead (with a toggle switch added) and other power leads in a simulated configuration to operate the ECM from an external power supply (part of the test instrumentation).

Table 6.8.2-3 shows which signals received each of the conducted susceptibility tests further detailed in the paragraphs below.

Table 6.8.2-3. Conducted Susceptibility Victim Test Summary Matrix

Victim Circuit	f) Conducted Susceptibility Power lines from -150 to +100v Pulses	g) Conducted Susceptibility Signal Lines from -60 to +40v pulses	h) Conducted Susceptibility 2Vp-p, 15Hz-150kHz	i) Conducted Susceptibility – Extended Audio, (30 kHz-250 kHz)	j) Conducted Susceptibility – Extended Audio, Signal Lines, Special Variant	k) Conducted Susceptibility – Bulk Current Injection, (26MHz-400 MHz) 1.0V p-p 106 dBuA	l) Power & Signal DC Loading +5 volts loaded starting at 5 ma and reducing the resistance to 0 Ohms. Started at 10 k Ohm and reduced the resistance to 0 Ohms.	m) Power Quality DC Voltage DC 13V, 14V, 15V, 16V, 13V, 12V, 11V, 10V, 9V, 8V, 7V, 6V, 5V, 4V, 13V, 14V, 15V, 16V, 17V and 18V	n) Power Quality – Voltage Dips (per ISO 16750-2) Voltage applied to the supply voltage lines. A dip is from 11 V to the dip voltage for the specified duration and then back to 11 V. The dip voltages are: 5.5 V, 5.0 V, 4.5 V, 4.0 V, 3.5 V and 3.0 V.	o) Power Quality Voltage Ripple 1) 1.2Vp-p on ECM 12V power input lines 2) 0.5Vp-p on 5V ECM power line 3) 2Vp-p, 15Hz-250kHz on ECM 12V power lines. 4) 4Vp-p, 15Hz-250kHz on ECM 12V power lines.
paragraph	6.8.3.1	6.8.3.2	6.8.3.3	6.8.3.4	6.8.3.5	6.8.3.6	6.8.3.7	6.8.3.8	6.8.3.9	6.8.3.10
ECM Ignition Power Lead	Yes		Yes	Yes		Yes		Yes	Yes	Yes
ECM Power	Yes		Yes	Yes		Yes		Yes	Yes	Yes
ECM Power	Yes		Yes	Yes		Yes		Yes	Yes	Yes
ECM Power	Yes		Yes	Yes		Yes		Yes	Yes	Yes
Reg 5V		Yes	Yes	Yes		Yes	Yes			Yes
Accel Pedal VPA1 Sensor		Yes	Yes	Yes	Yes with VPA2	Yes				
Throttle Body VTA1 Sensor		Yes	Yes	Yes		Yes				
Cruise Control Switch		Yes, 6.8.3.11	Yes	Yes		Yes				6.8.3.11
Crank Sensor		Yes	Yes	Yes		Yes				
Cam Sensor		Yes	Yes	Yes		Yes				
Mass Air Flow Sensor		Yes	Yes	Yes		Yes				
O2 Sensor		Yes	Yes	Yes		Yes				
Brake signal Input		Yes	Yes	Yes		Yes				
Brake signal Input NC		Yes	Yes	Yes		Yes				
Vehicle Speed Sensor to ECM		6.8.3.11				Yes				6.8.3.11
Drive Wheel Speed Sensor		6.8.3.11								6.8.3.11

6.8.3.1 Conducted Susceptibility Power Lines

ISO 7637-2 Conducted Transients (Column f)
This test was conducted in accordance with ISO 7637-2 adapted for testing on a vehicle with the following specifics:

The test level in volts is summarized as follows:

Test pulse	Test Level 1	Test Level 2	Test level 3	Number of pulses or test time	Burst cycle/ pulse rep rate
1	-50	-75	-100	50 pulses	3 sec
2a	+27	+50	+75	50 pulses	3 sec
3a	-50	-100	-150	5 min	100 ms
3b	+50	+75	+100	5 min	100 ms

The pulses were applied starting with Test Level 1 then Test Level 2, followed by Test Level 3 to the +12V battery supply leads of the ECM and to the Ign +12V supply lead of the ECM to the first vehicle. As there were no effects, in the interest of time, the remaining vehicles were tested only at Test Level 3. In particular, the 5V regulated voltage was monitored for fluctuations and any sign of interaction with the test pulses was documented.

6.8.3.2 Conducted Susceptibility Signal Lines

ISO 7637-3 Coupled Transients (Column g)
This test was conducted in accordance with Direct Capacitor Coupling method of ISO 7637-3 adapted for testing on a vehicle with the following specifics:

The test level in volts was as follows:

Test pulse	Test level	Test time	Pulse cycle time
Fast a	-60	2 min	100 ms
Fast b	+40	2 min	100 ms
Slow +	+30	2 min	
Slow -	- 30	2 min	

The test pulses were applied individually to the specified 5V regulated pin and each of the signal lines as shown in Table 6.8-3.

6.8.3.3 Conducted Susceptibility – Extended Audio, Signal Lines

Extended Audio frequency noise injection onto signal lines were transformer coupled and adapted from ISO 11452-10, (Column h). This test was conducted in accordance with Transformer Coupling methods adapted from ISO 11452-10 for testing on a vehicle with 2Vp-p, 15Hz-150 kHz applied to signal pins listed in Table 6.8.2-3.

6.8.3.4 Conducted Susceptibility – Extended Audio,

Extended Audio frequency noise injection onto signal lines were transformer coupled and adapted from ISO 11452-10, (Column I). This test was conducted in accordance with Transformer Coupling methods adapted from ISO 11452-10 for testing on a vehicle with 2Vp-p, 30 kHz-250 kHz applied to signal pins listed in Table 6.8.2-3.

6.8.3.5 Conducted Susceptibility Audio Frequency

SPECIAL TEST FOR Vehicle 12C ONLY – RIPPLE (Column j) :

The extended audio test was applied to the Accel Pedal Signal 1 alone, Accel Pedal Signal 2 alone, and to Accel Pedal Signal 1 and Accel Pedal Signal 2 simultaneously, and specifically to include 100 kHz.

6.8.3.6 Conducted Susceptibility

ISO 11452-3 BCI (Column k) The bulk current injection test was run from 26 MHz to 400 MHz with 100 frequency steps per decade and 2 sec minimum dwell. CW and 1 kHz 80 percent AM modulation was applied.

The test signal level was as follows:

26 MHz – 30 MHz: 106 dBuA
30 MHz – 400 MHz: $106 - 11*\frac{[\log(f\{\text{in MHz}\}) - \log(30)]}{[\log(400) - \log(30)]}$ dBuA

The test signal was applied to each individual connector bundle and, where practical, to all connector bundles simultaneously or as many together with the minimum number of groupings.

Test on vehicles 15C & 18C ONLY Column k For the frequency range of 10 kHz to 1 MHz, an AC test signal was applied (Direct Capacitor Coupled) to the leads specified:
Crankshaft Sensor (1.0V p-p)
Camshaft Sensor (1.0V p-p)

6.8.3.7 Power & Signal DC Loading

Test on vehicles 15C & 18C ONLY - 5V REGULATED OUTPUT LOAD TEST (Column l):

Using a suitably sized decade resistor box (or variable resistor), the 5V regulated output was loaded starting at 5 ma and reducing the resistance to 0 Ohms. The “5V” voltage versus external load resistance was recorded. Engine rpm variation and throttle angle variation was monitored and recorded as well as DTC generation using the Techstream diagnostic tool.

Test on vehicles 15C & 18C ONLY – Combination Meter Signal (Column l)

Using a suitably sized decade resistor box (or variable resistor), the combination meter signal to the ECM was loaded to determine effect on speed control system. Started at 10 Kohms and reduced the resistance to 0 Ohms. Recorded the "combination meter signal to the ECM voltage" versus external load resistance. Monitored and recorded engine rpm variation and throttle angle variation as well as DTC generation using the Techstream diagnostic tool.

6.8.3.8 DC Voltage Power Quality

Test on vehicles 15C & 18C ONLY – VOLTAGE RANGE TEST (Column m)

Using the combined power lead configuration and an external power supply, the voltage to the ECM was varied in the following sequence: 13V, 14V, 15V, 16V, 13V, 12V, 11V, 10V, 9V, 8V, 7V, 6V, 5V, 4V, 13V, 14V, 15V, 16V, 17V and 18V, and engine rpm variation and throttle angle variation was monitored and recorded as well as DTC generation using the Techstream diagnostic tool.

6.8.3.9 Power Quality AC Noise

ISO 16750-2 Electrical Environment (Columns n and o)
Power Quality tests included in ISO 16750-2 were tested as they were considered representative of the operating condition being investigated. These tests include Voltage ripple and Cranking Voltage tests.

The power supply leads were severed from the vehicle harness and connected together to form a single power supply point for the ECM.

Ripple test:
The extended audio frequency immunity test was run from 16 Hz to150 kHz. The 4V p-p test signal was applied to the combined 12V power leads.

Voltage dips test:
Voltage was applied to the supply voltage lines. A dip is from 11V to the dip voltage for the specified duration and then back to 11V. The dip voltages are: 5.5V, 5.0 V, 4.5 V, 4.0 V, 3.5V and 3.0V. Dips to each voltage level are for 100 µs, 1 ms, 10 ms and 500 ms durations. The DUT operation was monitored during the dip test and the interval time between dips was sufficient to verify normal DUT operation. At each dip voltage, the test was run through the range of dip durations.

Each supply voltage line was dipped individually.

Data: Basic report data as defined in respective referenced documents.

Functions observed and documented included throttle valve position, changes in engine speed, changes in vehicle speed, unexpected transmission gear shifts, changes of gauges, indicator lights or lighting levels of the instrument cluster, audible noises, or other unexpected behaviors.

Methods of observation included audible noise events within the vehicle and/or test chamber (e.g., vehicle engine noise) via fiber optic microphone, instrument panel monitoring via fiber optic TV camera, and dynamometer control system monitoring.

Data associated with observed events included plots of the test signal exposure level and tabulations of anomalies observed, frequency and the threshold level for each anomaly. DTCs were read periodically and when events were observed and recorded.

In particular, the ECM 5V reference voltage was monitored and any changes in voltage documented.

6.8.3.10 Power Quality Ripple

<u>ISO 11452-10 2009 Ripple on signal leads (Column o)</u>
The extended audio frequency immunity test adapted to test a complete vehicle was run from 16 Hz to 150 kHz.   The 2V p-p test signal was applied individually to each sensor lead, as shown in Table 6.8.2-3.

The extended audio frequency test signal was capacitor coupled to the 5V regulated output on one of the lines out of the ECM.

<u>Test on vehicles 15C & 18C ONLY – RIPPLE (Column o):</u>
For the frequency range of 150 kHz to 1 MHz, RF was applied (Direct Capacitor Coupled) to the leads specified:
Combined 12V power leads to a level of 1.2V p-p
5V regulated power leads was increased to a level of 0.5V p-p
Cruise Control Switch Input lead was to a level of 1.2V p-p

6.8.3.11 Cruise Control Test

<u>Test on vehicles 15C & 18C ONLY – Cruise Control Signal (Columns g, k, o):</u>
With the vehicle operating at temperature in cruise control at about 35 mph:
Applied the following test signals to these signal leads:

1) Cruise Control Switch lead

2) Speed signal from Combination meter to the EMC

3) Drive wheel speed sensor signal

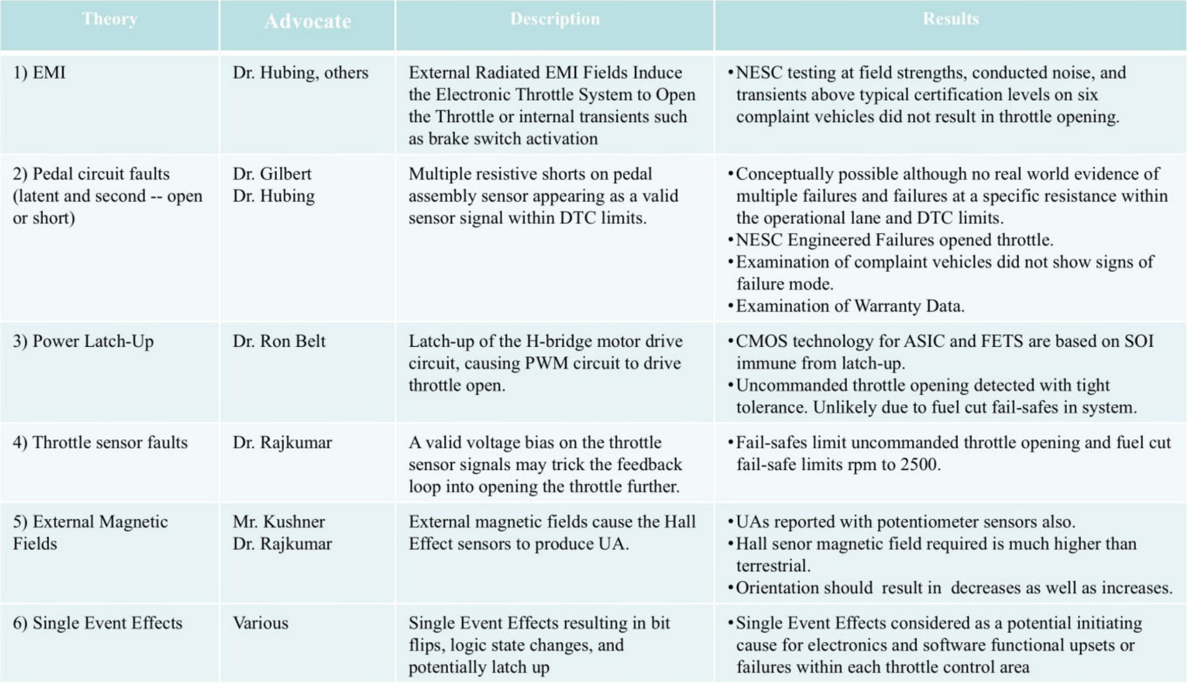
Applied the ISO 7637-3 transients capacitor coupled (Column g)
Applied the ISO 11452-10 test signal capacitor coupled up to 1.2V p-p (Column o)
Applied the extended range 150 kHz to 1 MHz test signal capacitor coupled up to 1.2V p-p

Determined threshold level for any interaction. (Column k)
Monitored and recorded engine rpm variation and throttle angle variation as well as DTC generation using the Techstream diagnostic tool.

6.9 External Theories

There were six main external theories that were supplied by NHTSA to be evaluated by the NESC team as shown in Table 6.9-1.

Table 6.9-1. External Theories



Theory	Advocate	Description	Results
1) EMI	Dr. Hubing, others	External Radiated EMI Fields Induce the Electronic Throttle System to Open the Throttle or internal transients such as brake switch activation	• NESC testing at field strengths, conducted noise, and transients above typical certification levels on six complaint vehicles did not result in throttle opening.
2) Pedal circuit faults (latent and second -- open or short)	Dr. Gilbert Dr. Hubing	Multiple resistive shorts on pedal assembly sensor appearing as a valid sensor signal within DTC limits.	• Conceptually possible although no real world evidence of multiple failures and failures at a specific resistance within the operational lane and DTC limits. • NESC Engineered Failures opened throttle. • Examination of complaint vehicles did not show signs of failure mode. • Examination of Warranty Data.
3) Power Latch-Up	Dr. Ron Belt	Latch-up of the H-bridge motor drive circuit, causing PWM circuit to drive throttle open.	• CMOS technology for ASIC and FETS are based on SOI immune from latch-up. • Uncommanded throttle opening detected with tight tolerance. Unlikely due to fuel cut fail-safes in system.
4) Throttle sensor faults	Dr. Rajkumar	A valid voltage bias on the throttle sensor signals may trick the feedback loop into opening the throttle further.	• Fail-safes limit uncommanded throttle opening and fuel cut fail-safe limits rpm to 2500.
5) External Magnetic Fields	Mr. Kushner Dr. Rajkumar	External magnetic fields cause the Hall Effect sensors to produce UA.	• UAs reported with potentiometer sensors also. • Hall senor magnetic field required is much higher than terrestrial. • Orientation should result in decreases as well as increases.
6) Single Event Effects	Various	Single Event Effects resulting in bit flips, logic state changes, and potentially latch up	• Single Event Effects considered as a potential initiating cause for electronics and software functional upsets or failures within each throttle control area

1. EMI. EMI could cause the kind of non-degrading momentary conditions described in the VOQ data without leaving physical evidence. However, EMI causes need a victim circuit within the electronics to initiate a throttle opening and a disturbing input needs to remain in place during the length of the UA. EMI analysis and testing is discussed in detail in section 6.8 above.

2. Pedal Circuit Faults. Accelerator pedal circuits provide a mechanism to command the throttle as long as both pedal circuits are perturbed without generating a DTC. The theory proposed by Dr. David Gilbert is that the ECM is susceptible to dual failures that affect both pedal sensor inputs that includes resistive shorts introduced to the pedal assembly sensors. Similarly, Professor Hubing proposed that failures on the pedal sensors supply voltage lines could cause a UA. Several other similar theories have been proposed. The

NESC team, as discussed in Section 6.6.2, investigated and demonstrated resistive shorts between the pedal sensor signal lines and power. The two pedal sensor signals were also shorted to each other through resistances below the fault detection threshold as described in Section 6.5.

3. Power Latchup. Another theory postulates that the circuit that drives the throttle drive motor can latchup. The NESC team investigated the effects of a latchup, described in Section 6.6, and determined that the motor drive circuit has protection against latchup conditions not only through the use of SOI technology, but also through multi-layers of failure detection and fail-safe modes. Dr. Belt proposed a theory that unsuppressed coil voltage transient may cause drive latch-up for the motor drive circuit. Results from the analysis and testing indicate that fail-safes limit uncommanded throttle to less than 5 degrees. Also, the NESC team performed EMI spike injection testing as discussed in Section 6.8 without causing a UA. Another protection is the fuel cut-off as described in Section 6.5.3.

4. Throttle Sensor Faults. A theory proposed by Dr. Raj Rajkumar suggests that a valid voltage bias, which could be caused by magnetic interference or sensor errors, on the throttle sensor signals could induce the throttle to open further. The NESC team performed EMI testing well beyond recommended certification levels, as discussed in Section 6.8, and investigated various failure conditions induced into the throttle sensor signals, discussed in Section 6.6.1. Results from the analysis and testing indicate that throttle assembly failures limit un-commanded throttle opening to less than 5 degrees.

5. External Magnetic Fields. Mr. Frank Kushner brought forward to the NESC a theory related to the possibility that solar activity accompanied by magnetic cracks in the earth’s magnetic shield could cause enough external magnetism at the Hall sensors to produce UA. The NESC team found that many UA VOQs occurred prior to the use of Hall sensors, with potentiometer sensor vehicles. Also, the magnetic field at which these sensors operate is more than one order of magnitude above typical terrestrial magnetic fields. Lastly, the NESC team found that a very strong local magnetic field that can cause sensor output increase would also be able to cause sensor output decrease depending on orientation.

6. Single Event Effects (SEEs) caused by energetic particles such as cosmic rays and protons can take on several forms. Single Event Upsets (SEUs) are soft errors, and non-destructive. They normally appear as transient pulses in logic or support circuitry, or as bit flips in memory cells or registers. Several types of hard errors, potentially destructive, can appear as Single Event Latchup (SEL). Latchup can result in a high operating current, above device specifications, and are typically cleared by a power reset. Other hard errors include Burnout of power MOSFETS, Gate Rupture, and frozen bits.

Specific failure modes including those potentially induced by single event effects are described with each of the throttle control functional areas of Section 6.6 and the Fishbone Analysis of Appendix B.

In general the throttle control electronics is protected from single event effects by the use of ASICs based on Silicon on Insulator technology and protective logic. In the event that throttle control electronics does fail, the layered defenses described in Section 6.5 such as low level DTCs, hardware level over current and over temperature protection, limp home modes, and fuel cut strategies guard the vehicle against UAs.

Processor and memory protection against single event effects includes EDAC on memory, data mirroring for critical variables, watch dog timer, and heartbeat functions between the two processors that check each other. Details are described in Section 6.6, and the Fishbone Analysis of Appendix B.

7.0 Findings, Observations, and NESC Recommendation

7.1 Findings

The majority of the engineering analysis associated with the study of UA was limited to MY 2005 Camry, L4 ETCS-i. Some analysis and testing was completed on MY 2005 L4 and V6, and a MY 2007 ETCS-i simulator. EMC testing was only performed on VOQ vehicles from MY 2002, 2003, 2004, and MY 2007. The following findings are based on this engineering analysis and testing.

F-1. No TMC vehicle was identified that could naturally and repeatedly reproduce large throttle opening UA effects for evaluation by the NESC team.

F-2. Safety features are designed into the TMC ETCS-i to guard against large throttle opening UA from single and some double ETCS-i failures. Multiple independent safety features include detecting failures and initiating safe modes, such as limp home modes and fuel cut strategies.

F-3. The NESC study and testing did not identify any electrical failures in the ETCS-i that impacted the braking system as designed.

a. 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.

b. 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 lb_f on the brake while the throttle is open up to 35 degrees (absolute), with a depleted vacuum assisted power brake system.

F-4. For pedal assembly failures to create large unintended throttle openings, failures need to mimic valid accelerator pedal signals.

a. 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 DTC.

b. Some first failures in dual failure scenarios of Hall Effect accelerator pedal systems might not be detectable by the ECM or via diagnostic data to the OBD interface.

c. A review of the warranty data does not indicate an elevated occurrence of pedal or ECM related DTCs relative to UA VOQs.

F-5. Destructive physical analysis of a failed pedal assembly from a VOQ vehicle with a DTC found a tin whisker[32] 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.

a. 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.

F-6. 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.

a. If the resistive short occurs while the vehicle is off, starting the vehicle with the accelerator pedal partially depressed will not trigger a diagnostic trouble code. When the accelerator is pushed slowly, the vehicle has a jumpy response, and is capable of full throttle without throttle brake override. When the accelerator pedal is pushed quickly, the fail-safe limp home mode is active including brake override.

b. If the resistive short occurs while driving, a DTC is declared along with a MIL, and fail-safe limp home mode is active including throttle brake override capability.

[32] 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/

c. If the key is cycled after the resistive short, the DTC and MIL remain. When the accelerator is pushed slowly, the vehicle has a jumpy response, and is capable of full throttle without throttle brake override. When the accelerator pedal is pushed quickly, the fail-safe limp home mode is active including brake override.

d. If the battery is disconnected with the resistive short, or the DTCs are otherwise cleared, DTCs will not return. When the accelerator is pushed slowly, the vehicle has a jumpy response and is capable of full throttle without throttle brake override. When the accelerator pedal is pushed quickly, the fail-safe limp home mode is active including throttle brake override.

F-7. Functional failures of the cruise control can result in 0.06 g's, or 2.12 kph/s, acceleration and may not generate a DTC; however, there are multiple methods for cancelling or turning off cruise control.

F-8. Functional failures of idle speed control, transmission control, VSC, and throttle control may result in throttle openings of less than 5 degrees above idle and may not generate a DTC. Per a NESC team request:

a. 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.

F-9. Comprehensive electromagnetic compatibility testing well beyond recommended certification levels was performed on six different TMC VOQ 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.

F-10. Extensive software testing and analysis was performed on TMC 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 UA were not found.

7.2 Observations

O-1. 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:

a. Shifting to neutral with the resulting high engine speed will not harm the vehicle.

b. Pumping the vacuum assist brakes can decrease their effectiveness.

c. Turning the vehicle off while driving may require a different sequence than when the vehicle is stopped and will not lock the steering wheel.

d. 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.

O-2. 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.

O-3. 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.

O-4. The Government-mandated (Environmental Protection Agency) DTCs are for emission control and are not mandated to cover safety critical failures.

O-5. 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.

a. NHTSA 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.

O-6. While not resulting in a design vulnerability, the MY 2005 Camry source code required unique code inspection tools, and manual inspections due to:

a. The TMC software development process uses a proprietary developed coding standard.

b. Industry standard static analysis tools provide automated code inspections based upon industry standard code implementations.

O-7. 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.

O-8. The available incident reporting databases are valuable for identifying potential vehicle symptoms related to UA events. However, voluntary reporting systems may not allow for accurate quantitative estimates of incident rates or statistical trends.

O-9. A review of HF literature related to UAs indicates that pedal misapplication remains an identified cause of some UAs. However, it is not possible to accurately estimate from available survey and laboratory data how frequently this error is an underlying cause.

O-10. 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.

O-11. 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.

7.3 NESC Recommendation

R-1. It is recommended that NHTSA consider whether additional study, government regulation, or policy is warranted based on the findings and observations within this report.

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

8.0 Alternate Views

There were no alternate views identified during the course of this assessment by the NESC team or the NESC Review Board (NRB) quorum.

9.0 Acronym List

Acronym	Description
A/CS	Air Conditioning Switch
ADC	Analog to Digital Conversion
APPS	accelerator pedal position sensor
ARC	Ames Research Center
ASIC	Application Specific Integrated Circuit
ASRS	Aviation Safety Reporting System
AUTOSAR	Automotive Open System Architecture
CARB	California Air Resources Board
CPU	Central processing unit
DC	direct current
DFRC	Dryden Flight Research Center
DI	Disable Interrupts
DOT	Department of Transportation
DTC	Diagnostic Trouble Code
ECM	Engine control module
ECU	Engine control unit
EDAC	error detection and correction
EDR	event data recorder
EEPROM	Electrically erasable programmable read-only memory
EI	Enable Interrupts
ELS1	Electronic Load Switch #1
EMC	electro-magnetic compatibility
EMI	electro-magnetic interference
ETC	electronic throttle control
ETCS-i	Electronic Throttle Control System-intelligent
FMEA	failure modes and effects matrix
FMVSS	Federal Motor Vehicle Safety Standards

Acronym	Description
GHz	Gigahertz
GSFC	Goddard Space Flight Center
HF	Human Factors
IC	Integrated circuit
ISC	Idle speed control
JPL	Jet Propulsion Laboratory
kHz	Kilohertz
KSC	Kennedy Space Center
LaRC	Langley Research Center
LV	light vehicle
MBD	Model-Based Design
MHz	Megahertz
MSFC	Marshall Space Flight Center
MY	model year
NCSL	Non-comment source lines
NESC	NASA Engineering and Safety Center
NSW	Neutral Switch
NHTSA	National Highway Traffic Safety Administration
NRB	NESC Review Board
OBD	On-board Diagnostic
PID	Proportional, Integral and Derivative
PWM	Pulse Width Modulation
RAM	random access memory
SEE	single event effect
SEL	single event latchup
SEU	single event upset
SGT	Stinger Ghaffarian Technologies
SMART	Swift Market Analysis Response Team
SPD	vehicle speed
SPICE	Simulation Program with Integrated Circuit Emphasis
SRAM	Static random access memory
STP	brake indicators

Acronym	Description
TDT	Technical Discipline Team
TEM	transverse Electro-Magnetic
THW	Coolant Water Temperature
TMC	Toyota Motor Corporation
TPS	throttle position sensor
TRAC	Vehicle traction control, a sub system of VSC
TSB	Technical Service Bulletins
UA	unintended acceleration
VOQ	Vehicle Owner’s Questionnaire
VRTC	Vehicle Research and Test Center
VSC	vehicle stability control
WCET	worst-case execution time
WDC	watchdog controller
WI	watchdog interrupt
WOT	wide open throttle