

Exponent®

Failure Analysis Associates

**Analysis of Toyota ETCS-i
System Hardware and
Software**



Analysis of Toyota ETCS-i System Hardware and Software

Prepared for

Steve St. Angelo, Chief Quality Officer
North American Quality Task Force
Toyota Motor Manufacturing
1001 Cherry Blossom Way
Georgetown, KY 40324

Prepared by

Exponent
149 Commonwealth Drive
Menlo Park, CA 94025

September 2012

© Exponent, Inc.

Contents

	<u>Page</u>
List of Figures	viii
List of Tables	xv
Acronyms and Abbreviations	xvii
Executive Summary	xix
1 Introduction	1
1.1 System Operation	2
1.2 Investigation Effort	5
1.3 Vehicle Model Selection	7
1.4 Report Summary	7
2 Approach	14
3 ETCS-i Basics and Operation	26
3.1 Introduction	26
3.2 Predecessor Cable System Design	27
3.3 ETCS-i	30
3.4 Fail-safes and Diagnostic Trouble Codes	31
3.5 Advantages of ETCS-i	33
3.6 Camry ETCS-i technology	34
4 Accelerator Pedal	37
4.1 Introduction	37
4.2 Pedal Circuit and Operation	38
4.2.1 Potentiometer based Pedals	39
4.2.2 Hall Effect sensor based pedals	43
4.2.3 Characterization Tests	47
4.3 Pedal Interaction with ETCS-i system	48
4.4 Accelerator Pedal Fail-safes	51

4.5	Pedal Position Learning and Related Vehicle Operating Modes	53
4.5.1	Narrow Lane	53
4.5.2	Wide Region	55
4.6	Pedal Circuit Failure Modes	56
4.6.1	Sensor Failures	56
4.6.2	Calibration	58
4.6.3	Electrical Noise	58
4.6.4	Resistive Faults and Contaminant Intrusion	60
4.6.5	Power Supply Variations	83
4.7	Multiple Failures	88
4.8	Resistive Faults between VPA1 and VPA2 and Vehicle Behavior on Restart	90
4.8.1	Non-linear Mode of Operation	93
4.9	Multiple Series Resistive Faults Leading to Low Supply Voltage	95
4.9.1	Low Voltage at Both Supply Terminals at Pedal End	96
4.9.2	Low Voltage Due to Power Supply Overload	97
4.10	Summary	97
5	Throttle Body	99
5.1	Introduction	99
5.2	Throttle Circuit and Operation	101
5.2.1	Potentiometer Based Throttles	102
5.2.2	Hall Effect Sensors	105
5.2.3	Characterization Tests	108
5.3	Throttle-Body Related Fail-Safes	109
5.4	Throttle Position Learning	111
5.5	Throttle Circuit Failure Modes	111
5.5.1	Sensor Failure Modes	112
5.5.2	Calibration	113
5.5.3	Electrical Noise	113
5.5.4	Resistive Faults	113
5.5.5	Power Supply Variations	127
5.5.6	Valve Sticking/Stuck Throttle Valve Condition	129
5.6	Multiple Failures	130
5.7	Summary	131

6	ECM Hardware	132
6.1	Introduction	133
6.2	ECM Variations	135
6.2.1	Number of Processors	135
6.3	ECM Construction and Testing	137
6.3.1	Housing Construction	137
6.3.2	ECM Operating and Storage Temperatures	140
6.3.3	ECM Tests	140
6.3.4	ECM Connectors	142
6.4	ECM Design and Theory of Operation	142
6.5	Filters and Protection Components	143
6.5.1	EMI/ESD Protection	143
6.5.2	Summary	145
6.6	Power Supply	145
6.6.1	Configuration	145
6.6.2	Filtering	147
6.6.3	Potential Failure Modes	147
6.6.4	Summary	153
6.7	Processors	153
6.7.1	Main Processor	153
6.7.2	Sub Processor	158
6.7.3	Failure Modes	159
6.7.4	Toyota Tin Whisker Testing	167
6.7.5	ECM Inspections and Testing	168
6.7.6	Summary	170
6.8	Analog to Digital Converter	170
6.8.1	Failure Modes	170
6.8.2	Summary	178
6.9	Throttle Motor Driver IC	178
6.9.1	Principle of H-Bridge Configuration	178
6.9.2	Logic Section	179
6.9.3	Failure Modes	180
6.9.4	Summary	187
6.10	Summary	188

7	ECM Software	190
7.1	Introduction	190
7.2	Approach	190
7.3	Flow Review	193
7.4	Static Analysis	193
7.4.1	Module Selection	194
7.4.2	PolySpace® Results	194
7.4.3	2002 V6 Camry	194
7.4.4	2007 V6 Camry	196
7.4.5	Summary	199
7.5	Mirroring	200
7.6	Error Correction Code (ECC)	201
7.7	Resource Locking	201
7.8	Test Data/Validation Report Review	202
7.9	Hardware-in-the-Loop Simulation	202
7.9.1	Input Variables	203
7.9.2	Tests performed	204
7.9.3	Summary	209
7.10	Summary	210
8	Other Hardware and System Level Considerations	212
8.1	Introduction	212
8.2	Electromagnetic Interference (EMI)	212
8.3	Latch-up	215
8.3.1	Causes of Latch-Up	215
8.3.2	Protection against Latch-Up	217
8.3.3	System Design	221
8.4	Software System Guards	223
8.4.1	Summary	230
8.5	Cruise Control System	231
8.5.1	Modes of Control	233
8.5.2	Cruise Control and Unintended Acceleration	236
8.6	System Level Protection Features	236

8.7	Software Failures	238
8.8	Resistive Faults	239
9	Parts Collected for Study	241
9.1	Introduction	241
9.2	Inspection of Field Components	241
9.2.1	Component Inspections and Resistive Contaminations	241
9.2.2	Component Inspections and Tin Whisker Investigations	244
9.2.3	Component Inspections and Continuity Measurements	246
9.3	Incident Vehicle Inspections	246
9.3.1	Vehicles Inspected	247
9.3.2	Findings	248
10	Connectors and Wiring	251
10.1	Introduction	251
10.2	ECM Connectors	251
10.2.1	Non-waterproof Connectors	251
10.2.2	Waterproof Connectors	255
10.2.3	Solder and Connector Pins	260
10.2.4	Wiring Insulation	260
10.3	Accelerator Pedal	261
10.3.1	Connector	261
10.3.2	Wiring Insulation	267
10.4	Throttle	268
10.4.1	Connector	269
10.4.2	Wiring Harness	271
11	Additional Issues	272
11.1	2007 Camry Engine “Hesitation” Complaints	272
11.2	Stalling of Corolla/Matrix Vehicles	273
11.3	Brake Override Systems	274
11.3.1	BOS Implementation	275
11.3.2	BOS Characterization Tests	277
11.3.3	Summary	281
12	Summary	283

Appendix A.	Accelerator Pedal Position Learning	286
Appendix B.	SOI Technology on Toyota ECMs	287
Appendix C.	Latch-up on Delphi ECMs	292
Appendix D.	Inspection of Field Components	294
Appendix E.	Pin-to-Pin Short Testing	295
Appendix F.	Tin Whisker Risk Assessment	296
Appendix G.	A/D Converter Testing	297
Appendix H.	BOS Characterization Tests	298

List of Figures

	<u>Page</u>
Figure 1. High-level block diagram of the throttle control system in a 2007 V6 Camry.	12
Figure 2. Rates of NHTSA complaints concerning unintended accelerations or surging of vehicle, or engine surges.	13
Figure 3. Primary classifications of potential ETCS-i system faults.	20
Figure 4. Components and subcategories of failures related to hardware.	20
Figure 5. Subcategories of software related faults.	21
Figure 6. Subcategories of system level faults.	21
Figure 7. Subcategories of failures related to pedal error.	22
Figure 8. Details of some parts of the investigation associated with electrical faults.	22
Figure 9. Details of some parts of the investigation associated with software faults.	23
Figure 10. Partial investigation details associated with characterizing system level interactions.	23
Figure 11. Partial investigation associated with pedal error.	24
Figure 12. Investigation overview.	25
Figure 13. Electronic Throttle Control System with Intelligence Function Diagram.	26
Figure 14. Cable-based throttle control design.	27
Figure 15. Pre-ETC throttle body system exploded view for a 2000 Tacoma L4 engine showing the accelerator cable and throttle position sensor connector.	28
Figure 16. 2004 Toyota Tacoma L4 pre-ETC throttle body mechanical linkage showing the accelerator pedal cable throttle valve control mechanism (white arrow) and the throttle position sensor (TPS – yellow arrow).	29
Figure 17. ECM from a 1998 Camry L4 (pre-ETCS-i).	29
Figure 18. Accelerator pedal for an ETCS-i equipped 2009 Toyota Corolla.	30
Figure 19. Throttle body from a 2003 Toyota Camry.	31
Figure 20. Aisan potentiometer pedal.	39
Figure 21. Aisan potentiometer pedal sensor.	40

Figure 22.	Denso potentiometer based pedal sensor.	40
Figure 23.	Nominal voltage outputs for a potentiometer-based pedal sensor as a function of rotation of the pedal sensor.	42
Figure 24.	Potentiometer pedal geometry (2006 Camry V6).	43
Figure 25.	Hall Effect sensor output characteristics.	44
Figure 26.	The Hall Effect sensor IC (yellow arrow) on a CTS pedal circuit containing the two independent Hall Effect sensors, and the resistors and the capacitors used for filtering and decoupling.	45
Figure 27.	Top and bottom surfaces of the CTS circuit board.	46
Figure 28.	Denso pedal permanent magnets (left) and Hall Effect sensors (right).	46
Figure 29.	X-ray image of Denso Pedal circuitry showing the two Hall Effect sensors and the electrical traces. Each Hall Effect sensor has a power supply and output terminal filter capacitor.	47
Figure 30.	Accelerator pedal sensor voltages as a function of pedal angle for selected Toyota and Lexus pedals.	48
Figure 31.	Hall Effect pedal sensor output as a function of accelerator pedal turning angle.	49
Figure 32.	Monitoring range and accuracy for pedals with parallel and diverging outputs.	50
Figure 33.	Signals with parallel slopes provide increased resolution by using a larger voltage range for the same pedal angle range.	51
Figure 34.	Allowable values for VPA1 and VPA2.	52
Figure 35.	Allowable values for VPA1 and VPA2 (2003 - 2005 Camry).	54
Figure 36.	Allowable VPA1 and VPA2 (2003 - 2005 Camry) with no pedal position learning at ignition on and no pedal position learning history.	55
Figure 37.	2004 Camry pedal position sensor after the injection of high current RF at EPA wire.	59
Figure 38.	CTS pedal circuit board. Arrow shows the pliable rubber gasket surrounding the rim providing a waterproof seal.	61
Figure 39.	Resistive fault between VPA1 and VPA2 resulting in the VPA1 voltage rising to VPA2. At idle, the deviation is the same for both, parallel or diverging systems.	66
Figure 40.	Single point resistive fault conditions that can affect VPA1 (the purple boxes indicate the location of the resistive fault for each fault condition).	67

Figure 41.	Potentiometer pedal output voltage with fault resistance to +5 Vdc terminal or ground terminal (GND).	68
Figure 42.	CTS pedal output voltage as a function of fault resistance to +5 Vdc or ground.	70
Figure 43.	Denso pedal output voltage as a function of fault resistance to +5 Vdc or ground.	72
Figure 44.	Resistive fault between VPA1 and VPA2 for a potentiometer pedal.	74
Figure 45.	Resistive fault between VPA1 and VPA2 for a CTS pedal.	75
Figure 46.	Resistive fault between VPA1 and VPA2 for a Denso pedal.	76
Figure 47.	Resistive fault in series with EPA for a potentiometer pedal.	79
Figure 48.	Resistive fault in series with EPA2 for a potentiometer pedal.	80
Figure 49.	Resistive fault in series with EPA for a CTS pedal.	81
Figure 50.	Resistive fault in series with EPA2 for a CTS pedal.	81
Figure 51.	Resistive fault in series with EPA for a Denso pedal.	82
Figure 52.	Resistive fault in series with EPA2 for a Denso pedal.	83
Figure 53.	Low voltage operation of the potentiometer pedal.	84
Figure 54.	Output voltage v. supply voltage for CTS Pedal.	85
Figure 55.	Output voltage v. supply voltage for Denso Pedal.	86
Figure 56.	Fault tree analysis of simultaneous pedal circuit resistive faults (Avalon).	89
Figure 57.	Flowchart of events for simultaneous pedal circuit resistive faults (Avalon).	90
Figure 58.	“Narrow” and “wide” regions of operation (2007 and later Camry vehicles).	91
Figure 59.	Potentiometer-based throttle position sensor in 2002 Camry L4 engine.	102
Figure 60.	Throttle body for 2002 Camry V6 (top), throttle position sensor connections (lower left), potentiometers on throttle position sensor (lower right).	103
Figure 61.	Potentiometer based throttle circuit response. X-axis angles refer to angles along the perimeter of the potentiometer (drawing on the left), not the throttle angle, which is approximately 10° smaller.	104
Figure 62.	Throttle body of a 2007 Toyota V6 Camry showing the throttle valve (blue arrow) and gear housing (red arrow).	105

Figure 63.	2007 Toyota L4 Camry gear housing sectioned to show the gearing (red arrow): Hall Effect sensors (yellow arrow), and throttle motor housing (green arrow).	105
Figure 64.	Gear housing sectioned to show the gears coupled to the throttle motor. Permanent magnets which provide the magnetic field sensed by the Hall Effect sensors are shown by the blue arrow.	106
Figure 65.	Hall Effect sensor output characteristics.	107
Figure 66.	Throttle motor voltage and current. Engine at idle. The feedback loop adjusts the duty cycle in real-time.	108
Figure 67.	Test Condition #3: Engine ON, accelerator pedal in different positions.	109
Figure 68.	Single point resistive fault conditions that affect throttle position sensor output.	114
Figure 69.	Throttle position sensor output voltages as a function of a fault resistance between VTA1 and the ground terminal for a potentiometer-based throttle position sensor.	116
Figure 70.	Throttle position sensor output voltage as a function of a fault resistance between VTA1 and the ground terminal for a Hall Effect throttle position sensor.	117
Figure 71.	Resistive fault between VTA1 and VTA2 for a potentiometer based throttle.	118
Figure 72.	Resistive fault between VTA1 and VTA2 for a Hall Effect sensor based throttle.	119
Figure 73.	Throttle position sensor output voltages as a function of a fault resistance between VTA1 and the +5 Vdc terminal for a potentiometer based throttle position sensor.	120
Figure 74.	Throttle position sensor output voltage as a function of a fault resistance between VTA1 and the +5 Vdc terminal for a Hall Effect throttle position sensor.	121
Figure 75.	Resistive fault in series with the VTA1 signal between the throttle circuit and the ECM for a potentiometer based throttle position sensor.	123
Figure 76.	Resistive fault in series with the VTA1 signal between the throttle circuit and the ECM for a Hall Effect sensor based throttle position sensor.	124
Figure 77.	Potentiometer based throttle output as a function of series resistance on the VCTA line.	125
Figure 78.	Hall Effect sensor based throttle output as a function of resistance in series with the power supply voltage signals (VCTA).	126

Figure 79.	Throttle plate stuck partially open by inserting a metal object under the throttle plate.	130
Figure 80.	High level ECM configuration for control of the throttle assembly (*In some vehicles the A/D converter is physically located on the same ASIC as one of the Processors).	133
Figure 81.	System level hardware configuration for Camry vehicles equipped with ETCS-i.	136
Figure 82.	ECM from 2007 V6 Camry with waterproof housing.	138
Figure 83.	ECM for a 2002 V6 Camry as installed behind the glove box (left). ECM with connectors removed (right).	139
Figure 84.	Conformal coating on some ECMs. The FTIR analysis indicates that the coating is a straight acrylic polymer.	140
Figure 85.	Overload V-I Characteristic of the main +5 Vdc Supply for a 2005 Camry V6.	149
Figure 86.	Software architecture for throttle control on the 2007 V6 Camry.	154
Figure 87.	Watchdogs and processor failures (WDC: watchdog counter).	163
Figure 88.	Principle of H-bridge motor drive (U1, U2, U3 and U4 represent MOSFETs in this diagram).	179
Figure 89.	Approach to software analysis.	191
Figure 90.	System features that protect against EMI and the system response to EMI induced failures.	213
Figure 91.	SOI CMOS inverter circuit.	218
Figure 92.	Cross section of bipolar transistors and CMOS transistor fabricated in the SOI BiCMOS process.	220
Figure 93.	System features that protect against latch-up and the system response to a latch-up condition.	223
Figure 94.	System configuration.	224
Figure 95.	Coverage provided by System Guard 1 (light green block).	226
Figure 96.	Coverage provided by System Guard 2 (light green box) when the vehicle is being driven.	229
Figure 97.	Cruise control system configuration.	232
Figure 98.	Cruise control operation.	234
Figure 99.	System level protection features.	237

Figure 100.	Levels of protection against software system failures.	238
Figure 101.	Levels of protection against resistive faults.	240
Figure 102.	Used vehicle parts were acquired for resistive contamination testing.	242
Figure 103.	Insulation test method to measure surface resistances due to contaminants.	243
Figure 104	Wiring harness of Toyota Tacoma including the pedal, ECM and the intermediate connector.	244
Figure 105.	View of ECM installation in a 2003 V6 Camry. Interior trim and the glove box have been removed so the ECM can be seen.	253
Figure 106.	Male ECM connector for a 2002 V6 Camry. The ECM cover has been removed. Yellow arrow points to the gold-plated pins used for the throttle signals. Blue arrow shows the gold-plated pins used for the accelerator pedal position sensor signals. Green arrows show the tin-plated pins used for the power signals sent to the throttle motor.	253
Figure 107.	Female, non-waterproof ECM connector for a 2002 V6 Camry. The wires are individually insulated, bundled, protected and routed away from penetrations. Yellow arrows show the locking mechanism.	254
Figure 108.	Male portion of the ECM connector.	255
Figure 109.	ECM connector. Arrows show the gray connector locking mechanism.	256
Figure 110.	ECM connector in locked position and portion of wiring harness. Yellow arrow shows locking gray connector in locked position.	257
Figure 111.	ECM female connector assembly for the large connector. A rubber gasket (red arrow) on the rim of the connector housing is used to make the connection waterproof.	258
Figure 112.	Wiring harness side of female ECM connector. Yellow arrow shows that each connector lead is insulated and protected by a polymeric grommet that helps make the connector waterproof and provides another layer of electrical isolation between sockets.	259
Figure 113.	Male portion of the ECM connector showing the gold plated and tin plated pins.	260
Figure 114.	Potentiometer pedal (male) connector.	262
Figure 115.	Hall Effect sensor pedal (male) connector configuration.	262
Figure 116.	Potentiometer pedal connector. Each connector lead is insulated and protected by a polymeric grommet (red arrow) that helps make the connector waterproof and provides another layer of electrical isolation between sockets. Another polymeric grommet seals the two halves of the connector (yellow arrow). The female connector pin receptacles are	

	recessed. There are two barriers surrounding the VPA1 and VPA2 pins (green arrows).	263
Figure 117.	Hall Effect pedal connector. Each connector lead is insulated and protected by a polymeric grommet that helps make the connector waterproof and provides another layer of electrical isolation between the sockets.	263
Figure 118.	Pedal Assembly Connector- female (left) and male (right). Blue arrow shows the gasket. Red arrows show the interlocking clasp.	265
Figure 119.	Potted and sectioned Hall Effect based accelerator pedal sensor connector.	265
Figure 120.	Each connector lead is insulated and protected by a polymeric grommet that helps make the connector waterproof and provides another layer of electrical isolation between sockets.	266
Figure 121.	Accelerator pedal connector design used on certain models showing certain features, such as individual wire polymeric grommet seals, polymeric seal between connector halves, and interlocking connector.	267
Figure 122.	Connector pins on the throttle body connector. From left to right: VTA1, VCTA, VTA2, ETA, M+, M1. The signal pins are gold plated.	269
Figure 123.	Male portion of the throttle body connector with gold plated signal pins and tin plated power pins.	270
Figure 124.	Close-up of female portion of the throttle body connector with the orange sealing grommet visible.	270
Figure 125.	Each throttle body connector lead is insulated and protected by a polymeric grommet that helps make the connector waterproof and provides another layer of electrical isolation between sockets.	271
Figure 126.	Die photograph and cross section image of die type 1.	287
Figure 127.	Type 2 die photograph and cross section image.	288
Figure 128.	Type 3 die photos and cross section image.	289
Figure 129.	Type 1 die photographs and cross section image.	290
Figure 130.	Type 2 die photographs and cross section image.	291

List of Tables

	<u>Page</u>
Table 1. Software architecture (throttle control system) design of Toyota and Lexus vehicles. (grey cells - power train manager based architecture)	35
Table 2. DTC associated with pedal faults	51
Table 3. Vehicle response to a latch-up of the Hall Effect sensors in the pedal circuit	57
Table 4. Resistive faults between VPA1 and VPA2 for the three pedal types and region of operation	94
Table 5. DTC associated with throttle body related faults	110
Table 6. Vehicle response to a latch-up of the Hall Effect sensors in the throttle circuit	112
Table 7. Power supply voltages used on selected Toyota vehicles	146
Table 8. Vehicle response to abnormal operation of components on the ECM due to an over-voltage condition	151
Table 9. Vehicle response to abnormal operation of the processors on the ECM	161
Table 10. 2002 V6 Camry primary throttle modules code verification summary	195
Table 11. 2007 V6 Camry primary throttle modules code verification summary	198
Table 12. 2007 V6 Camry PolySpace [®] ISC code verification summary	199
Table 13. Variables set at startup	203
Table 14. List of ECMs examined by Exponent	220
Table 15. Mitigations and possible consequences of component latch-up	221
Table 16. DTCs related to the cruise control system	235
Table 17. List of parts used by Exponent for inspections regarding the matter of tin whiskers	244
Table 18. List of inspected vehicles with reported unintended acceleration incidents	247
Table 19. Technology used on inspected vehicles	248
Table 20. Vehicles with BOS	276
Table 21. BOS activation and applied brake pedal force	278

Table 22.	BOS activation and order of pedal depression	279
Table 23.	BOS activation and vehicle speed threshold	279
Table 24.	BOS activation time delay, accelerator pedal position and throttle request angle	280

Acronyms and Abbreviations

A	Amperes
ABS	Anti-lock Brake System
A/D Converter	Analog-to-Digital Converter
ASIC	Application Specific Integrated Circuit
ASRT	Assertion
AUTOSAR	AUTomotive Open System ARchitecture
CAN	Controller Area Network
CARB	California Air Resources Board
CMOS	Complementary Metal-Oxide-Semiconductor
COR	Correctness condition
CPU	Central Processing Unit
DTC	Diagnostic Trouble Code
ECC	Error Correcting Codes
ECM	Engine Control Module
ECT	Electronically Controlled Transmission
EDS	Energy Dispersive Spectroscopy
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
ETCS-i	Electronic Throttle Control System - Intelligent
FTIR	Fourier Transform Infrared Spectroscopy
GUI	Graphical User Interface
HILS	Hardware in the Loop Simulator
IAT	Intake Air Temperature
IDP	Illegal Dereference of a Pointer
IC	Integrated Circuit
IRV	Initialized Return Value
ISC	Idle Speed Control
k-NTC	Known Non Terminating Call
LED	Light Emitting Diode
MAF	Mass Air Flow
MIL	Malfunction Indicator Lamp
MOSFET	Metal Oxide Semiconductor Field Effect Transistor
NHTSA	National Highway Traffic Safety Administration
NIP	Non-Initialized Pointer
NIV	Non-Initialized Variable
NMOS	N-channel Metal-Oxide-Semiconductor
NTC	Non Terminating Call
NTL	Non Terminating Loop
OBAI	Out of Bounds Array Index
OVFL/UNFL	Overflow or Underflow
PID	Proportional-Integral-Derivative
PMOS	P-channel Metal-Oxide-Semiconductor
PWM	Pulse Width Modulated

RAM	Random Access Memory
ROM	Read Only Memory
SAE	Society of Automotive Engineers
SCR	Silicon-Controlled Rectifier
SEM	Scanning Electron Microscopy
SHF	Shift amount out of bounds or left operand of left shift
SOI	Silicon-On-Insulator
TPS	Throttle Position Sensor
UA	Uncommanded Acceleration
UNP	Unreachable Procedure
UNR	Unreachable code
V	Volts
VSC	Vehicle Stability Control
WDC	Watchdog Counter
ZDV	Zero Division

Executive Summary

Exponent investigated whether Toyota vehicles equipped with electronic throttle control technology could accelerate in an uncommanded manner (uncommanded acceleration). Older generations of engines used a throttle cable to mechanically control the throttle valve opening and engine power. Engines with electronic throttle control, including Toyota's Electronic Throttle Control - Intelligent (ETCS-i) technology, use an electric motor on the throttle body controlled by microprocessors in place of the throttle cable. Exponent's investigation into uncommanded acceleration (UA) involved determining whether any ETCS-i component, alone or in conjunction with other components, could develop a condition or fault(s) that would cause the vehicle to experience sustained and uncontrolled acceleration without being so commanded (e.g., by depression of the accelerator pedal or by cruise control commands).¹

Exponent's investigation has determined that the Toyota ETCS-i is designed with a network of protection to detect both component and system failure(s) and transition the vehicle to a "fail-safe" mode. Individual component failures, such as that of a pedal position sensor, are detected at the component level and an appropriate fail-safe action is initiated. System level safeguards are activated in the event of a failure of the dedicated hardware and software fail-safes to detect fault conditions at the component level.

Toyota's ETCS-i contains three system-level software safeguards. The sole purpose of these safeguards is to limit the throttle valve opening for any given accelerator pedal position. These safeguards continually monitor the pedal and throttle positions and can force the engine into a fail-safe mode of operation on detection of a fault.

Exponent's investigation concluded that the electronics and software in Toyota vehicles equipped with ETCS-i do not have any single points of failure that can result in UA. In addition, Exponent did not identify credible non-single point software or electronic failures that would result in UA in Toyota vehicles equipped with ETCS-i.

¹ Unintended acceleration is a term that has been generally used in describing reported incidents where customers reported unexpected vehicle or engine speed increases. This is different from uncommanded acceleration defined above. In this report, UA represents uncommanded acceleration, not unintended acceleration.

Specifically, Exponent's investigation of the Toyota ETCS-i concluded that:

- The vehicle's electronics, software and overall system design employ a network of protection designed and incorporated in the vehicle that transitions the vehicle to one of the designed fail-safe modes in the event the engine control module (ECM) detects a sub-system or component failure.
- Exponent's evaluation and testing determined that realistic environmental levels of electromagnetic interference (EMI) would not cause UA in Toyota vehicles. The vehicles' electronics and software employ multiple strategies that minimize interference from electrical noise and mitigate its possible consequences.
- "Latch-up"² was eliminated as a potential root cause for reported incidents of unintended acceleration. The multiple levels of protection in the ETCS-i and its network of safety, that include electronics, software, and the use of silicon-on-insulator technology in many integrated circuits, prevent latch-up (if it could occur) from resulting in UA.
- The system design implements several approaches for mitigating concerns associated with either the formation of tin whiskers, or the growth of tin whiskers that are sufficiently long and have the potential for shorting adjacent conductors³. These include, among others:
 1. Conformal coating of electrical printed circuit boards. The coating acts as a mechanical barrier against tin whisker growth;
 2. Encasing of certain components in an epoxy potting compound, which also acts as a mechanical barrier against tin whisker growth;

² A circuit is said to be "latched up" when it ceases to function normally and remains in a fixed state until power is cycled. (John Daintith. "latch-up." A Dictionary of Computing, 2004. <http://www.encyclopedia.com/doc/1O11-latchup.html>)

³ Only one manufacturer of one type of pedal position sensor had a concern with tin whisker formation. Detailed studies on the response of this sensor, along with reviews of warranty data, could not attribute reported incidents of unintended acceleration to tin whiskers.

3. Employment of electrical connections that either do not contain tin, such as gold and nickel-palladium-gold coatings, or that use techniques known to limit whisker growth.
- An analysis of the system level software safeguards indicates that, in addition to the dedicated component level safeguards that monitor and respond to the various subsystem and component malfunctions, system level software safeguards are designed to detect failures of the system and to prevent the vehicle from experiencing UA either due to single-point failures or due to the failure of multiple software modules and/or electronic subsystems. The response of these safeguards was investigated in detail using hardware-in-the-loop-simulations; our results indicated that these safeguards are designed to ensure that the allowable deviation in the throttle opening angle under the simultaneous failure of multiple sub-systems is limited.⁴
 - A line-by-line review of the sections of the source code relevant to throttle control was performed to identify possible logical or functional bugs that would result in UA; no such faults were found.
 - Exponent reviewed the software test documents from Toyota and performed static analysis on source code to identify runtime errors that would result in UA; no such errors were found.
 - The analysis and testing performed on components and vehicles indicated that the system design prevents the vehicle from experiencing UA in the event of:
 - Component failures within sub-systems
 - Power supply anomalies such as over-voltage, under-voltage etc.
 - Realistic resistive faults due to contaminants, tin whiskers, etc.

⁴ A review of the system design and testing indicated that outside idle mode, the throttle opening angle cannot differ by more than ■■■ from the non-linearly corrected pedal request angle after accounting for the electrical load requests (via the idle speed control module). In absolute terms, this means that the throttle opening angle cannot differ by more than ■■■ from the non-linearly corrected pedal request under the absolute worst case scenario without triggering a DTC which transitions the vehicle to the fail-safe mode.

Based on our investigation, Exponent concluded that the electronics and software were not the root cause of the reported incidents of unintended acceleration in the Toyota vehicles we evaluated.

1 Introduction

Exponent investigated potential causes for elevated unintended acceleration complaint rates in Toyota vehicles equipped with ETCS-i⁵ technology. As part of its investigation, Exponent evaluated the potential of UA as it might relate to electrical hardware and/or software malfunctions, or due to electromagnetic interference (EMI). The focus of this report will be on the analysis and testing performed on the software and hardware systems in Toyota Camry vehicles.

The scope of Exponent's investigation was sufficiently broad that it was appropriate to address different aspects of the investigation in separate reports. For example, the analysis of electromagnetic interference (EMI) had several facets that included a review of the hardware design and an extensive test program. The test program for EMI is covered in a separate, stand-alone report, while the hardware design aspects are reported here. Similarly, aspects of pedal configuration and testing in the context of cabin design, analyses of event data recorder (crash recorder) performance, and other topics were addressed in different reports.

Exponent's approach to this investigation was multifaceted and included:

- Detailed reviews of the software and hardware and the interaction between the hardware and software
- Analysis of new and used components and testing of vehicles purchased on the open market.
- Inspection and testing of customer vehicles alleged to have been involved in unintended acceleration incidents.
- Subjecting components and vehicles were to a variety of tests and simulated fault conditions, including exposure to extreme electromagnetic interference, in both laboratory and real-world environments.

⁵ Electronic Throttle Control System with intelligence

Within each section of this report, the discussion focuses on the testing and results that address the primary concerns of that section. If a particular test or analysis was performed on multiple components or vehicles, a sample of the test or analysis is presented in the section to minimize redundancy. Note that findings and conclusions described at the end of each section are based on collective and accumulated knowledge about the behavior of the component in the context of how the ETCS-i system and vehicle behave as a whole. This report is not intended to be either a chronology of testing, or contain a description of every test and test finding. Results that are helpful to explain the operation of the vehicle under various fault conditions are discussed in the report.

Toyota vehicles equipped with ETCS-i systems have evolved through several generations, though they share some common features. The Toyota Camry was selected as a primary vehicle for this investigation because it was a high production volume vehicle with elevated rates of unintended acceleration complaints, and was the subject of multiple investigations by the National Highway Traffic Safety Administration (NHTSA). Exponent performed a detailed review of ETCS-i-equipped Camry vehicle system designs to identify the various hardware and software system operating modes, interconnecting design methodologies, and fail-safe systems. This report will detail the design of Camry's throttle control system, discussing the various sub-systems and their response to failure conditions. This report will also summarize the signal flow from the accelerator pedals to the microprocessors, the throttle motor driver IC on the ECM and the PWM voltage to the throttle motor, along with the feedback signals from the throttle position sensor.

1.1 System Operation

Toyota vehicles equipped with ETCS-i technology utilize electronic throttle control with numerous sensors to ensure that the throttle is at its commanded position at any given time. The desired throttle valve opening angle,⁶ which controls airflow to the engine's cylinders, and therefore the power of the vehicle, is calculated by the engine control module (ECM). The primary input is either the position of the accelerator pedal or the vehicle's cruise control

⁶ Also called the 'throttle angle' in this report.

system. The final throttle angle is adjusted using “feedback” signals from a number of engine systems including the throttle valve assembly itself. For example, engaging the air conditioner creates a demand for engine power, thus requiring an increase in throttle angle so power to the wheels is not reduced. In addition, engine sensors monitor the vehicle’s operating condition and optimize the vehicle’s response (including power, fuel economy, knock sensing and emissions) based on these feedback signals. Finally, safety systems such as stability control and traction control can affect throttle angle, adjusting power to the wheels to assist the driver in maintaining control of the vehicle. The processing of these signals is performed by the ECM, which, in addition to controlling the throttle valve opening, also sends signals to control fuel injection, and spark and valve timing.

In the 2007 V6 Toyota Camry, depressing the accelerator pedal results in increases in the voltage from two independent sensors mounted on the accelerator pedal. The electronic control module (ECM) receives and analyzes data from these and other sensors and sends commands to different components, such as the throttle body. The commands sent by the ECM to the throttle body control the angular position of the throttle valve and therefore the rate at which air is drawn into the engine. Two throttle position sensors monitor the position of the throttle valve, sending voltage signals back to the ECM about the current throttle position. The result is a closed loop system where the feedback signals from the two throttle position sensors are used by the ECM to ensure that the throttle valve is at the desired position. A failure of the closed loop system to move the throttle valve to the desired position triggers a DTC and transitions the vehicle to the fail-safe mode.

Figure 1 is a high-level block diagram of the throttle control system for a 2007 V6 Camry, depicting the sub-components that determine the throttle opening position. As shown in Figure 1, the ECM controls the vehicle engine output power using information from various sensors and consists of a number of integrated circuits (ICs) and active and passive discrete components.

Depending on the vehicle model, an ECM may contain two or more microprocessors. In ECMs containing more than two microprocessors, two of the microprocessors are directly involved in throttle control. One of the microprocessors processes all the throttle opening requests (hereinafter the “Main” processor) from various sources (for example, the pedal position,

electrical loads, cruise control system settings, etc.) and sends a command signal to the throttle motor driver integrated circuit (IC). A second microprocessor acts as a fail-safe processor (hereinafter called the “Sub” processor), monitoring the operation of the Main processor and other subsystems.

The throttle motor driver IC processes the signal from the Main processor and sends a pulse-width-modulated (PWM) voltage to the throttle motor. The throttle motor can be activated to both open and close the throttle valve. In addition, the throttle body contains springs that force the throttle valve to a nearly closed position if no power is sent to the motor.

The springs in the throttle motor assembly set the throttle opening angle to approximately 6° when no current is drawn by the throttle motor, or when the vehicle enters a “fail-safe” mode of operation. The throttle motor is commanded to oppose a spring force to reduce the throttle opening angle to approximately 2° to 4° when the vehicle is at idle. When current to the throttle motor is shut off (such as during fail-safe operation), the return spring sets the throttle opening angle to approximately 6° , limiting maximum engine power.⁷

Figure 1 also shows the signal path from the accelerator pedal to the throttle motor for a 2007 V6 Camry. The main components depicted in Figure 1 are:

1. The accelerator pedal contains two Hall Effect sensors that convert pedal position to voltage signals which are sent to the ECM. Earlier versions of the accelerator pedal position sensors were potentiometers.
2. The analog voltage signals are filtered immediately after entering the ECM
3. An analog-to-digital (A/D) converter digitizes the filtered analog signals for the Main processor.
4. The Main processor processes the digital signals and provides the Motor Activation Control signal and Motor Duty Cycle control signal to the throttle motor driver IC. Thus, the Main CPU produces two levels of control signals:

⁷ See section 3.4 for further details.

- a. On/off control for the throttle motor power supply
 - b. Motor Control - speed, direction of rotation (clockwise or counterclockwise), and duty cycle.
5. The Sub processor also provides two types of control signals to the throttle motor driver IC for controlling the throttle motor. These include:
- a. On/off control for the throttle motor power supply
 - b. On/off control for the throttle motor
6. The throttle motor driver IC responds to the signals from the two processors and supplies control signals to the Motor Supply MOSFET and also supplies a pulse-width modulated (PWM) voltage to the power MOSFET H-Bridge.
7. The throttle motor is driven by a bi-directional PWM output from the power H-bridge configuration formed by the MOSFETs in the throttle motor driver IC and external MOSFETs.
8. The output of the power H-Bridge is supplied to the throttle motor for speed and direction control. The throttle motor controls the opening of the throttle valve.⁸

Exponent's investigation focused on studying the design and architecture of the ETCS-i system, identifying failure modes, and determining the system response to identified failure modes by analyzing the system's design (hardware and/or software), through testing in the laboratory, and/or through simulating failures and studying the system response in operating vehicles.

1.2 Investigation Effort

Exponent was not constrained in its approach to the investigation of potential root causes for unintended acceleration by either tasks or areas, nor was Exponent restricted to analyzing

⁸ In fail-safe mode, the current to the throttle motor is cut off and the return spring sets the throttle angle to 6°.

particular interpretations of unintended acceleration. Exponent's approach to this task was multifaceted and included design reviews (both hardware and software), software code analysis and verification, laboratory testing, vehicle testing of both exemplar vehicles and vehicles purchased from the open market, inspections of parts retrieved from the field and inspections of vehicles that were alleged to have been involved in incidents of unintended acceleration.

The hardware and software review focused on identifying potential mechanisms that could lead to unintended increases in the throttle valve angle. It is recognized that modest increases in engine speed can be obtained by means other than increasing throttle angle, such as varying the air/fuel ratio, spark and the intake/exhaust valve timing etc. However, the mechanical shaft power of the engine is primarily limited by the rate of combustion air flowing through the throttle valve, so the generation of significant additional power will necessarily be associated with increases in the throttle valve angle. Some conditions that result in the onset of a diagnostic trouble code⁹ (DTC) may exhibit momentary increases in engine RPM before the onset of the DTC and before the vehicle enters the fail-safe mode.

Exponent performed testing on multiple Toyota vehicles of various model years. Camry models transitioned from cable based throttle systems to ETCS-i based systems starting with the 2002 model year.

Our analysis was performed by conducting individual investigations of each of the following sub-systems of the ETCS-i, as well as system-level performance.

- Accelerator pedal
- Processors
- Throttle Motor Driver
- Throttle Body (including throttle motor and throttle position sensors)

⁹ Toyota vehicles set diagnostic trouble codes (DTCs) when a fault is detected in one or more sub-systems. The response of the vehicle to a DTC depends upon the type of fault that occurs and the classification of the fault in the software. This is discussed in detail in section 3.4.

- Analog to Digital Converter
- Power Supply
- Wiring & Connectors.

This report describes each of the sub-systems and summarizes the results of the analysis performed on each subsystem. The latter portion of the report discusses and summarizes the system level analysis performed and details the levels of protection employed by the Camry ETCS-i system.

1.3 Vehicle Model Selection

The Toyota Camry was selected for more detailed study because of its high sales, significant publicity surrounding alleged unintended acceleration events, the NHTSA investigations into unintended acceleration, and elevated unintended acceleration complaint rates based on Exponent's analysis of complaints in NHTSA's database. Figure 2 shows the complaint rates for different models of Toyota and Lexus vehicles equipped with ETCS-i technology, with Camry complaint rates highlighted.

1.4 Report Summary

This report is structured as follows:

- Chapter 1 is this introduction
- Chapter 2 will discuss the approach taken by Exponent for the investigation, providing a description of the methodologies used by Exponent to address various areas of our inquiry.
- Chapter 3 will discuss Toyota's ETCS-i system in greater detail, providing an explanation on how the system operates and how it differs from designs prior to the introduction of electronic throttle control in vehicles. In addition to a

discussion of the features of the ETCS-i system, the chapter will also discuss self-diagnosis and fail-safe checking performed by the ETCS-i system.

- Chapter 4 will focus on the accelerator pedal circuit. The accelerator pedal circuit is the component that translates movement of the accelerator pedal into voltages used by the ECM to determine desired engine output. The accelerator pedal circuit designs have changed over the years, originally employing potentiometers before transitioning to contact-less Hall Effect-based sensing technology. This chapter will discuss the following:
 - Theory of operation of both potentiometer-based pedal designs and Hall Effect-based pedal designs
 - A discussion of the various failure modes of the accelerator pedal circuit and the vehicle response to these failure modes. This will include a discussion of the pedal circuit design and results of testing performed to simulate pedal circuit failures.
 - A discussion of the advantages and disadvantages on the selection of a parallel slope design for the pedal circuit operation compared to a diverging slope design.
 - A summary of the results of the pedal circuit analysis performed by Exponent.
- Chapter 5 will focus on the throttle system. This will include the throttle motor which drives the throttle valve and the throttle valve position circuitry. The throttle position sensor is attached to the throttle body and provides feedback to the ECM about the angular position of the throttle valve. Throttle position sensors predate the use of electronic throttle controls, providing information that was used by the ECM for better engine control, such as fuel injection. For vehicles with electronic throttle control, the throttle position sensor provides feedback to the ECM about valve angle, allowing the ECM to make adjustments in the current driving the throttle

motor to achieve the desired throttle angle. As with the accelerator pedal position sensors, throttle position circuit designs have also transitioned from potentiometer-based to Hall Effect-sensor based designs. This chapter will discuss the following:

- Theory of operation of both potentiometer-based throttle circuit designs and Hall Effect-based throttle circuit designs
 - A discussion of the various failure modes of the throttle circuit (the throttle motor and the throttle position sensor circuit) and the vehicle response to these failure modes. This will include a summary of the results of the testing performed to simulate throttle related failures both in the laboratory and in Toyota vehicles.
 - A summary of the results of the throttle analysis performed by Exponent.
- Chapter 6 will focus on the Engine Control Module (ECM). The ECM is the “brains” of the ETCS-i system, and uses signals from the accelerator pedal sensors and other sensors to control the engine, including controlling the throttle valve. This chapter will provide a high level summary of the ECM design, including a discussion on the protection circuitry and its response to both internal and external failure conditions. The chapter will discuss the following:
 - Toyota Camry ECM system design
 - ECM circuitry failure modes and vehicle response
 - Summary of testing performed on the ECM
 - Summary of the results of the ECM analysis performed by Exponent.
 - Chapter 7 will discuss the ETCS-i system software design. This will include a summary of the testing performed by Exponent to evaluate the software,

including the results of the static testing and testing performed using the hardware in the loop simulator (HILS).

- Summary of the software based fail-safes incorporated in the ETCS-i design.
- Chapter 8 will provide a system-level analysis of the ETCS-i system. Failure modes and fault conditions that could potentially affect sub-systems (for example tin whiskers). This chapter will include the following:
 - Discussion of the Camry ETCS-i system as it relates to response to electrical noise. This will include a discussion of the system response to EMI and the results of the EMI testing performed by Exponent.
 - A discussion of latch-up and the effect of latch-up on the Toyota Camry ETCS-i system.
 - A summary of the protection safeguards incorporated in the Toyota ETCS-i system (at both the design and manufacturing level) and the response of these safeguards to component/system failures.
 - Summary of system response to software failures at both the module and system level.
 - A discussion of the Toyota Camry cruise control system and the response of the vehicle to a failure of the cruise control system
- Chapter 9 will summarize Exponent's analysis of Toyota parts collected for study and testing. Both new and used parts were acquired by Exponent for this analysis. This chapter will also summarize the results of Exponent's inspections of six customer vehicles that were alleged to have experienced an unintended acceleration event.
- Chapter 10 will provide a summary of the hardware used to electrically interconnect the ETCS-i sub-systems, and Exponent's investigation of the

construction of the connectors and design and manufacturing of the wiring harnesses.

- Chapter 11 summarizes the analysis performed by Exponent into one cause for the elevated complaint counts associated with the 2007 and early 2008 model year Camry vehicles. This chapter will also summarize root causes for the stalling of Corolla and Matrix vehicles.
- Chapter 12 will provide a summary of the results of Exponent's investigation.

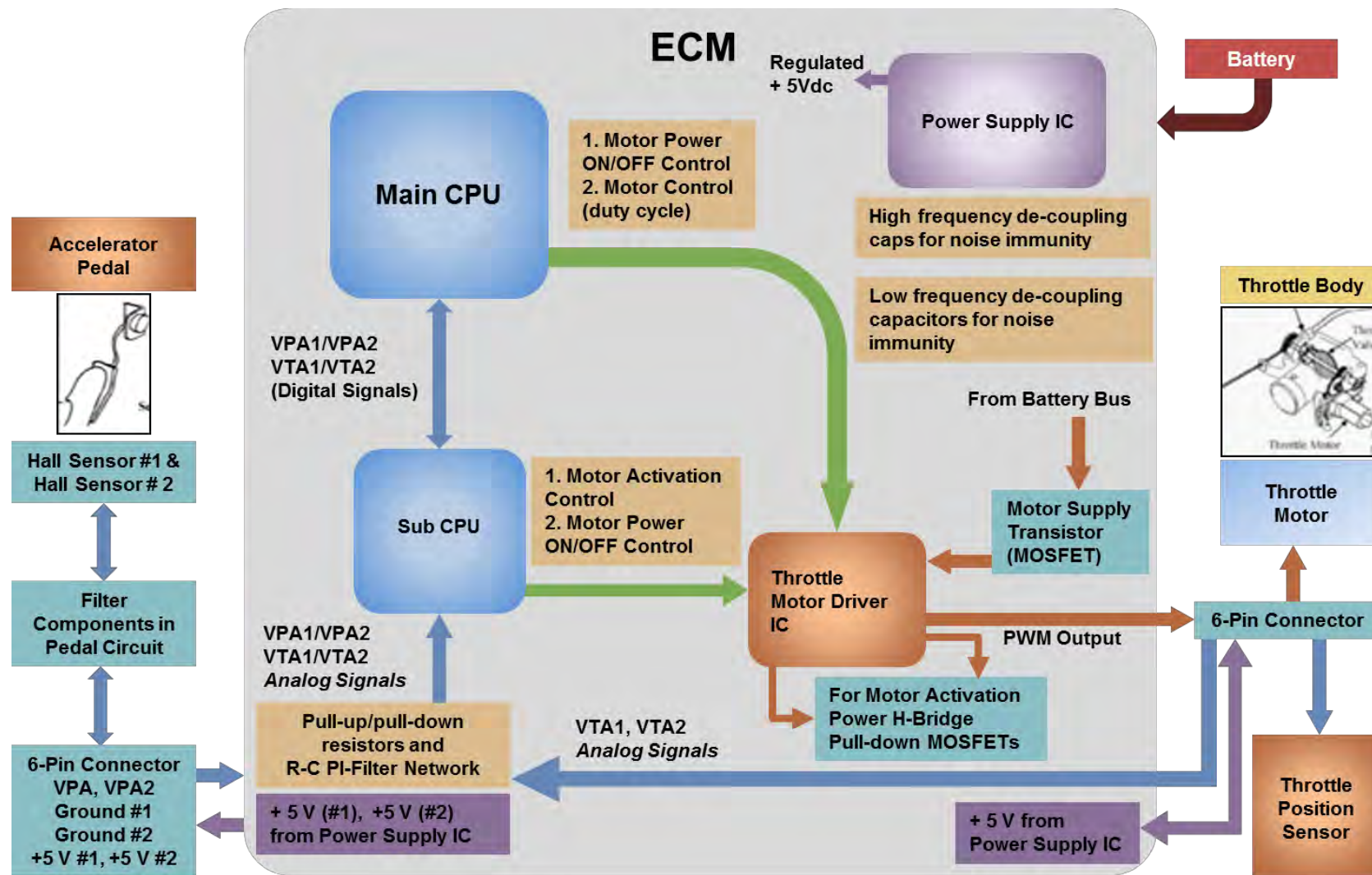


Figure 1. High-level block diagram of the throttle control system in a 2007 V6 Camry.

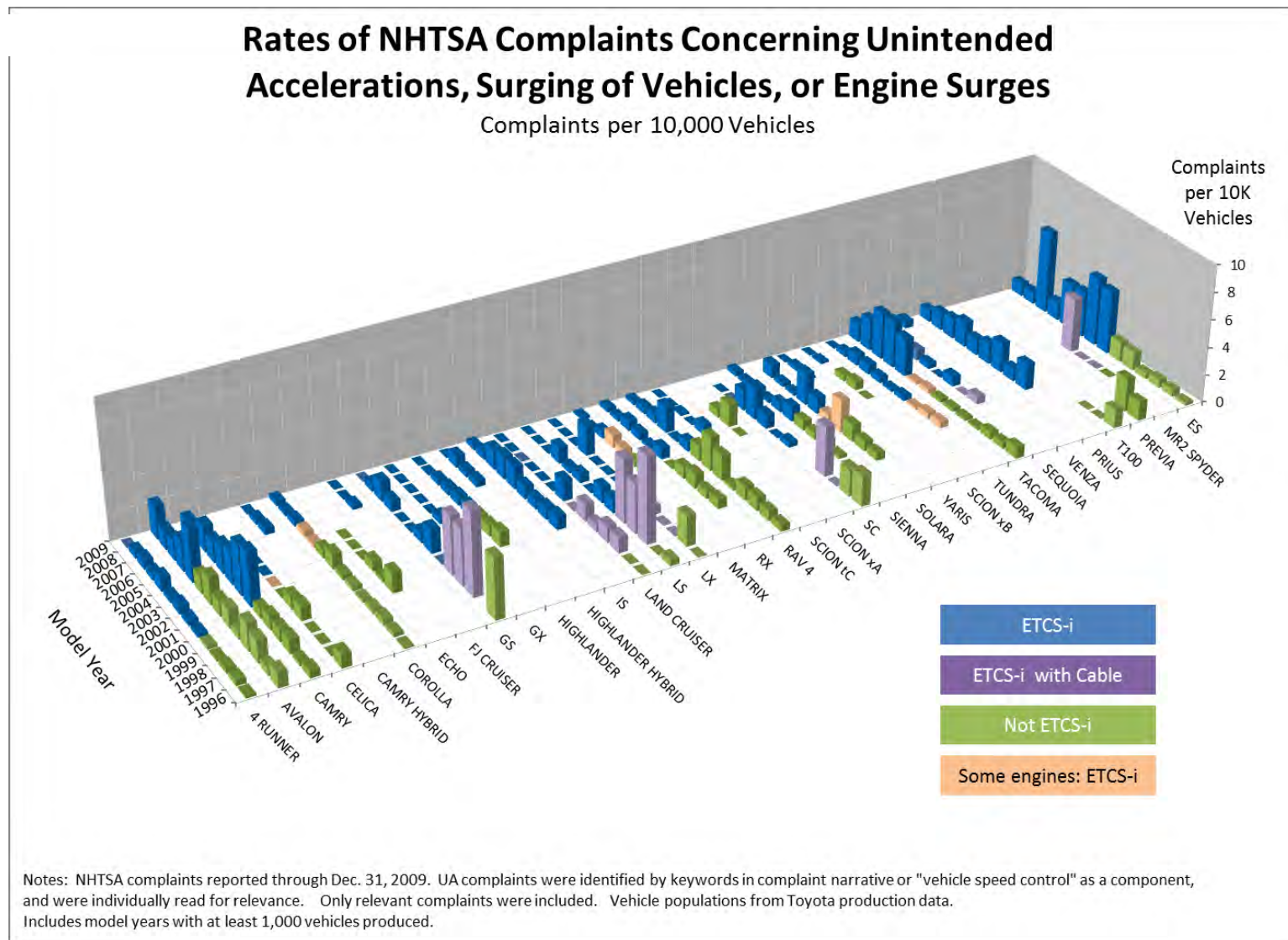


Figure 2. Rates of NHTSA complaints concerning unintended accelerations or surging of vehicle, or engine surges.

2 Approach

Exponent's methodology for investigating potential root causes of product failures uses both traditional and problem-specific methodologies to identify and address relevant scenarios and hypotheses on an ongoing basis. This ensures the flexibility to examine potential causes as they might arise, while still providing a comprehensive basis for the investigation. Exponent's investigation was necessarily multi-disciplined, incorporating contributions from many engineering and scientific disciplines. This process was facilitated by Exponent's ability to draw upon an in-house staff of 600+ degreed professionals representing expertise in more than 90 different scientific and engineering disciplines, many of which are directly relevant to the design and manufacturing of modern vehicles. These include electrical engineering, electronic and integrated circuit engineering, mechanical engineering, materials science, vehicle engineering, vehicle testing, computer science, software engineering, risk analysis, human factors, and biomechanics. In addition to Exponent's team of technical professionals with advanced degrees, our experimental facilities include state-of-the-art analytical laboratories, automotive test facilities including a two-mile test track, and access to independent test facilities around the world. Exponent's Quality Management System is certified to ISO 9001.

Unintended acceleration is a term that has been generally used in describing incidents where customers reported unexpected vehicle or engine speed increases. This is different from uncommanded acceleration, where the vehicle or engine speed increases significantly when the accelerator pedal is not depressed by any means,¹⁰ or the cruise control has not been so commanded by the driver. In this report, UA represents uncommanded acceleration, not unintended acceleration. For example, a floor mat entrapment of the pedal causing the vehicle to accelerate would be an incident of unintended acceleration, but not uncommanded acceleration, since the ECM cannot differentiate whether the pedal was depressed by a foot or a

¹⁰ We are excluding cases where the engine speed increases because of a transmission downshift, operation of accessories, cold idle operation, etc. Whereas some drivers may report accelerations that they consider are greater than expected for a given pedal position, if the acceleration is mitigated when the pedal is released to the idle position, it would be of lesser concern since speed is demonstrably controllable by changing the pedal position.

floor mat. Historically, a number of definitions have been put forth for the term unintended acceleration. Some of these definitions include:

- “..sudden acceleration incidents" (SAI) are defined for the purposes of this report as unintended, unexpected, high-power accelerations from a stationary position or from a very low initial speed accompanied by an apparent loss of braking effectiveness. In the typical scenario, the incident begins at the moment of shifting to "Drive" or "Reverse" from "Park”.¹¹
- “The term ‘sudden acceleration’ (SA) has been used (and misused) to describe vehicle events involving any unintended speed increase. However, the term properly refers to an ‘unintended, unexpected, high-power acceleration from a stationary position or a very low initial speed accompanied by an apparent loss of braking effectiveness.’ The definition includes ‘braking effectiveness’ because operators experiencing a SA incident typically allege they were pressing on the brake pedal and the vehicle would not stop. ‘Sudden acceleration’ does not describe unintended acceleration events that begin after vehicles have reached intended roadway speeds.”¹²
- “...‘unintended acceleration’ refers to unintended, unrequested, uncontrollable, and/or unexplained acceleration of a subject vehicle, and to the failure of a vehicle's engine to return to idle when the driver takes his or her foot off of the accelerator pedal or raises his or her foot to a position where the engine ordinarily would return to idle, regardless of the alleged or determined cause of the acceleration or failure to decelerate or return to idle and regardless of the speed at which the event allegedly took place. Unintended acceleration thus is broader than interference between the

¹¹ Pollard and Sussman, “An Examination of Sudden Acceleration,” January 1989 (Study for NHTSA), p. 1.

¹² Federal Register Volume 68, No. 183, September 22, 2003: NHSTA Denial of Petition, 2.1 “Sudden Acceleration (SA)”

accelerator pedal and driver's side floor mat and sticking accelerator pedals with levers made of a particular plastic(s)."¹³

- "... 'unintended acceleration' also refers to the occurrence of any degree of acceleration that the vehicle driver did not purposely cause to occur. Contrast this with the term 'sudden acceleration incident,' which refers to unintended, unexpected, high-power accelerations from a stationary position or a very low initial speed accompanied by an apparent loss of braking effectiveness. (*An Examination of Sudden Acceleration*, DOT-TSB, NHTSA_90-1 at v). As used here, unintended acceleration is a very broad term and encompasses sudden acceleration as well as incidents at higher speeds and incidents where brakes were partially or fully effective, including occurrences such as pedal entrapment by floor mats at full throttle and high speeds and incidents of less throttle openings at various speeds."¹⁴

The first step in Exponent's investigation was to develop a technical statement of the task. This involved a study of the design and operation of Toyota's ETCS-i system and a review of the concerns and complaints in reported incidents of unintended acceleration (including complaints stored in the National Highway Transportation Safety Administration's VOQ database). Exponent's investigation goal was to identify hardware and/or software related characteristics or realistic fault conditions that could result in vehicle behavior consistent with the reported incidents of unintended acceleration. Reported incidents of unintended acceleration often described vehicle acceleration without driver input for a duration beyond the reaction times of the vehicle's fail-safe mechanisms¹⁵. As a result, Exponent's Toyota investigation was focused on identifying any vehicle characteristics or realistic fault conditions that could lead to vehicle acceleration consistent with these types of reported incidents. This is because engine power is limited by the amount of combustion air drawn into the cylinders, which is in turn limited by the size of the throttle valve opening. In the absence of a significant opening of the throttle valve, the engine power and consequently the vehicle's acceleration are limited. This task statement

¹³ NHSTA Opening Resume for RQ10003, 2/16/10, p. 2.

¹⁴ NHSTA "Technical Assessment of Toyota Electronic Throttle Control (ETC) systems", February 2011

¹⁵ Vehicle fail-safe mechanisms are triggered at approximately 500 ms. upon detection of a fault condition.

necessarily focused on conditions that could cause the throttle valve to open without a command from the pedal sensors.

Review of unintended acceleration complaints in the NHTSA database indicated that drivers typically claimed that they were either unable to or had difficulty controlling the speed of their vehicle despite brake application. A sustained throttle valve opening was thus included in Exponent's task definition, since a momentary opening of the throttle valve would not provide sufficient time for the vehicle speed to change. Also, small ECM adjustments to the throttle valve opening are constantly made by design to balance changes in power demand, operating conditions, fuel economy and emissions requirements, so modest changes in engine speed are expected.¹⁶

Many tools and methodologies are available to investigators looking to identify the root causes of a failure. These tools, which include fishbone diagrams and fault tree analyses, can be valuable and useful, particularly for organizing or structuring an investigation. Exponent uses a process that includes facets of several of these tools, placing an emphasis on approaching the investigation from different vantage points. Exponent's experience has honed this approach and found it to be very effective as it capitalizes on our strengths as a multi-disciplinary organization. This approach is illustrated diagrammatically in Figure 3 through Figure 11.

Figure 3 shows the basic categories of potential faults that can affect the ETCS-i system. Each block represents a range of possible faults. As an example, Figure 4 shows components associated with "Hardware Malfunctions", and basic subcategories of potential faults related to each component. Note that the primary components of the ETCS-i system are the throttle body (incorporating the throttle valve and throttle position sensor), the ECM (which directly controls the throttle valve), the accelerator pedal, and the wiring and connectors between these components. Figure 4 illustrates the relationship between these components, and a variety of potential fault-inducing conditions or failure modes, such as electromagnetic interference (EMI) or latch-up, that could potentially affect the component or lead to an uncommanded opening of

¹⁶ In vehicles equipped with ETCS-i technology, in addition to the accelerator pedal, electrical loads (for example air conditioner) in the vehicle can also cause an increase in the throttle opening angle. This increase is generally in the 1° to 2° range (see section 6.7 for further details) and is limited to less than ■° for the studied vehicles.

the throttle valve. The same fault-inducing conditions, such as EMI, can have an effect on multiple components as illustrated in Figure 5. Similarly, Figure 5, Figure 6 and Figure 7 show basic faults and failure modes encompassed by software issues, system level issues, and pedal error issues respectively. Pedal error, also known as pedal misapplication, would be classified as resulting in unintended acceleration, rather than uncommanded acceleration. However, a study was performed on the pedal positions, geometries, force - displacement characteristics, and other pedal-vehicle characteristics and is discussed in a separate report.

Within each sub-category of fault or failure mode shown in Figure 5 through Figure 7, there are additional considerations for analyses and testing. Electrical faults, software faults, interactions with other systems, and pedal error are shown in Figure 8 through Figure 11, respectively. These diagrams illustrate a greater level of detail. For each particular fault or failure mode (shown in these figures as a salmon-colored box), external factors within the domain of the specific concern were considered. For the example shown in Figure 8, external factors that might lead to hardware faults on the ECM include such elements as EMI. These are factors that could be hypothesized to result in UA through some process where the ECM operation or the signals it receives are physically affected.

Surrounding the external factors box in Figure 8 are aspects or protective measures that are part of the design or operation of the vehicle. These aspects and protective measures were included in the external factors evaluations, and in the testing design.

Figure 8 also contains a box with specific analyses and tests that were designed to evaluate external factors. For example, tin whisker analysis was the first line item analyzed. The tin whiskers investigation was to determine whether certain hardware designs were susceptible to tin whiskers of a size that could potentially result in shorting and whether such shorting could lead to UA. The initial tin whisker evaluation was performed by a team of engineers and scientists with expertise in automotive engineering, electrical engineering, printed circuit board fabrication, and tin whisker formation. Exponent retained a world-renowned expert in tin whisker formation, Dr. Craig Hillman, CEO of DfR Solutions, to assist in the evaluation. Exponent assembled documentation, communicated with component manufacturers, and acquired new and used components for evaluation. The results were periodically reviewed and

additional tests and analyses performed as necessary. Thus, the single element “tin whisker” in Figure 8 encompasses an entire program of study and testing that was part of the larger analyses of faults that can affect the ECM, throttle body, accelerator pedal, wiring and connectors. Such a process, adapted as appropriate for the issue, was applied to each area of investigation.

Figure 12 is an overview, combining major considerations into a single graphic. Some additional external factors, tests and analyses not shown in the prior figures are included in this graphic. The advantage of this approach is that the interactions between tests, concerns, and the ETCS-i system are transparent. Interactions not previously considered can be detected and evaluated. As knowledge about Toyota’s ETCS-i system grows, this approach provides great flexibility for adding concerns, analyses and tests, and understanding protective features. Further, many experiments were useful in evaluating more than one aspect of the ETCS-i system’s performance, and thus could address concerns arising in multiple subcategories of concerns.

Testing and analyses generally comprised multiple experiments or analyses performed on multiple components in multiple vehicles. Sound engineering judgment guided the selection of components, vehicles and tests. For example, model year 2007 and later Camrys are equipped with accelerator pedals using Hall Effect sensors from one of two manufacturers. For stress testing of the accelerator pedals, it was important to include pedals from both manufacturers since they used different electronics in their pedals. However, pedal electronics did not undergo any known significant changes from 2007 forward, so it was unnecessary to differentiate pedal model years. Factors, such as temperature and humidity, were evaluated for problem creation such as latch-up, open circuits, and tin whisker or dendrite growth.

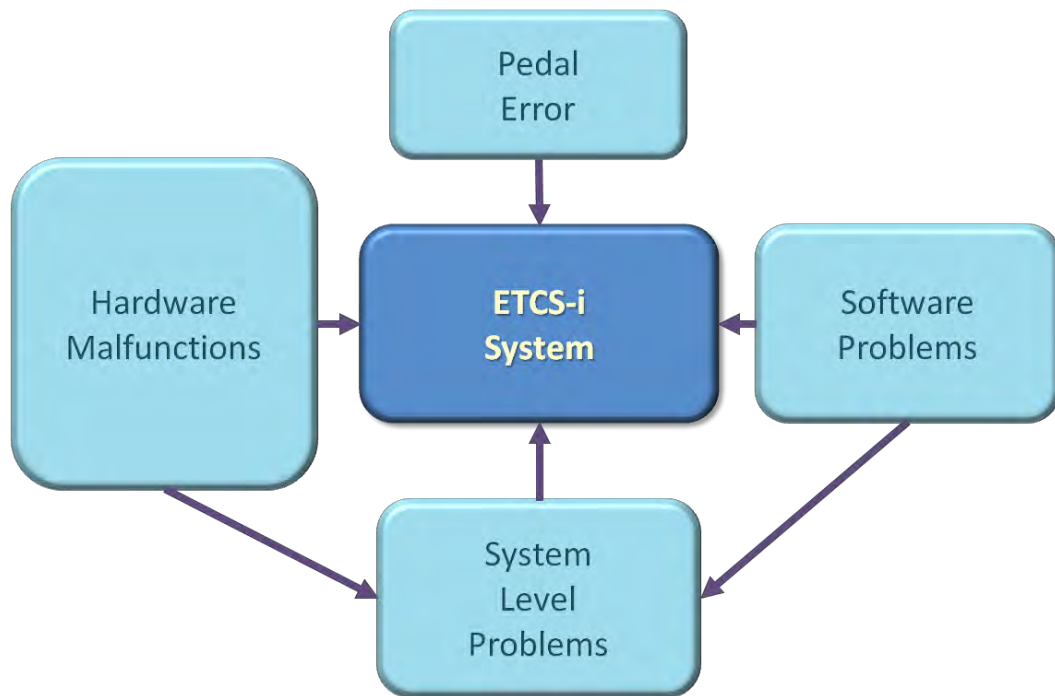


Figure 3. Primary classifications of potential ETCS-i system faults.

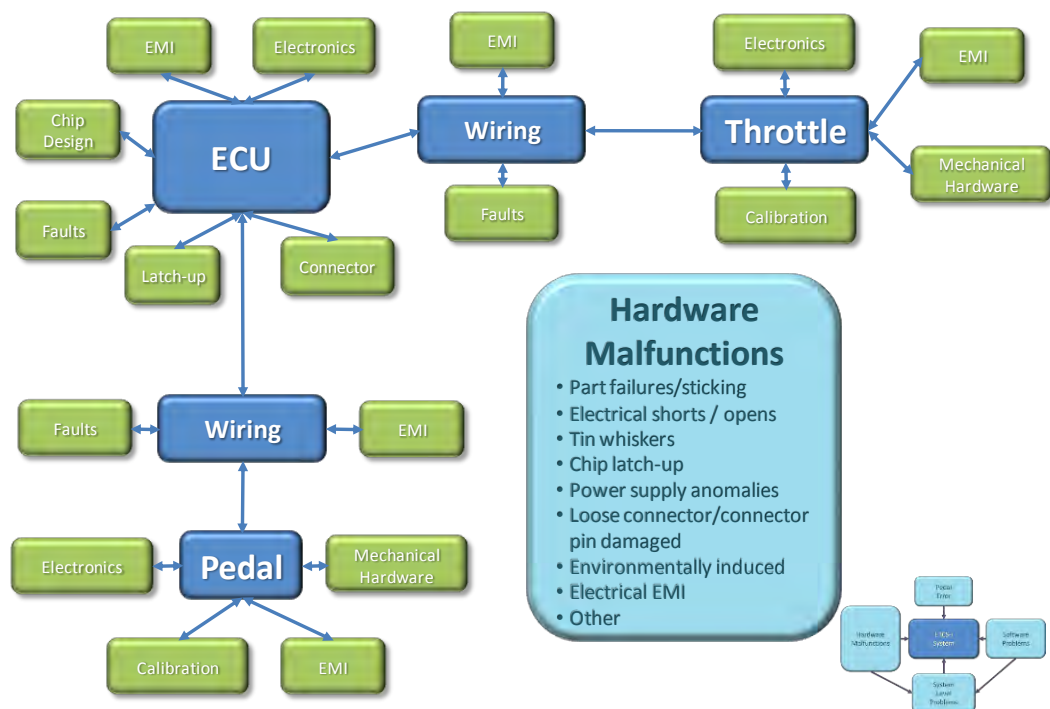


Figure 4. Components and subcategories of failures related to hardware.

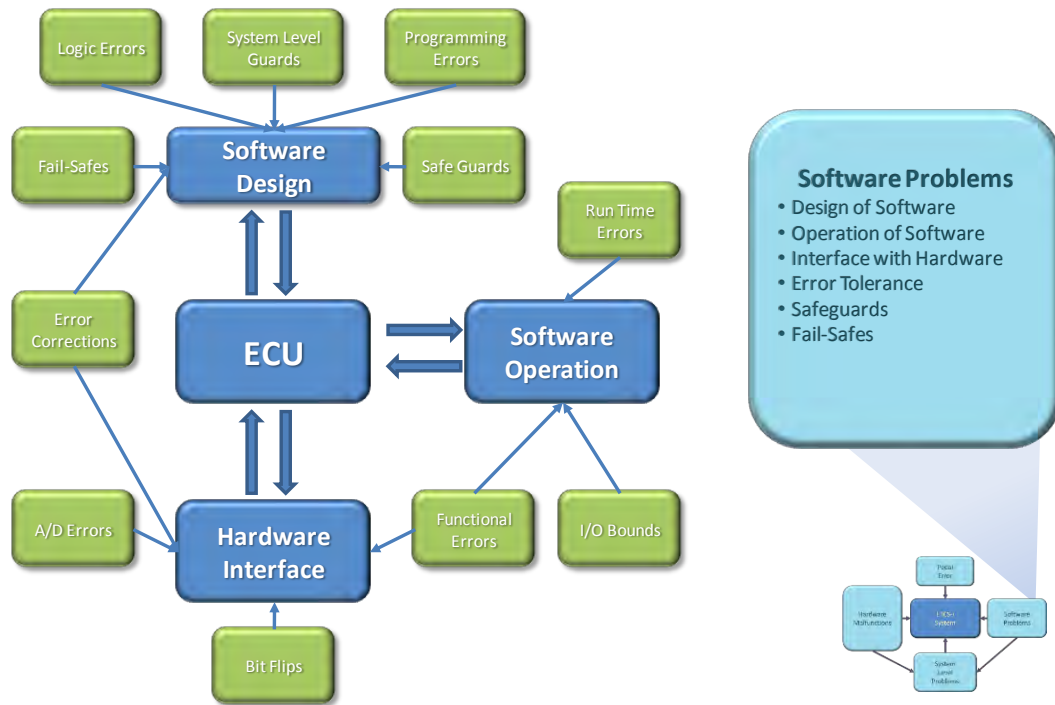


Figure 5. Subcategories of software related faults.

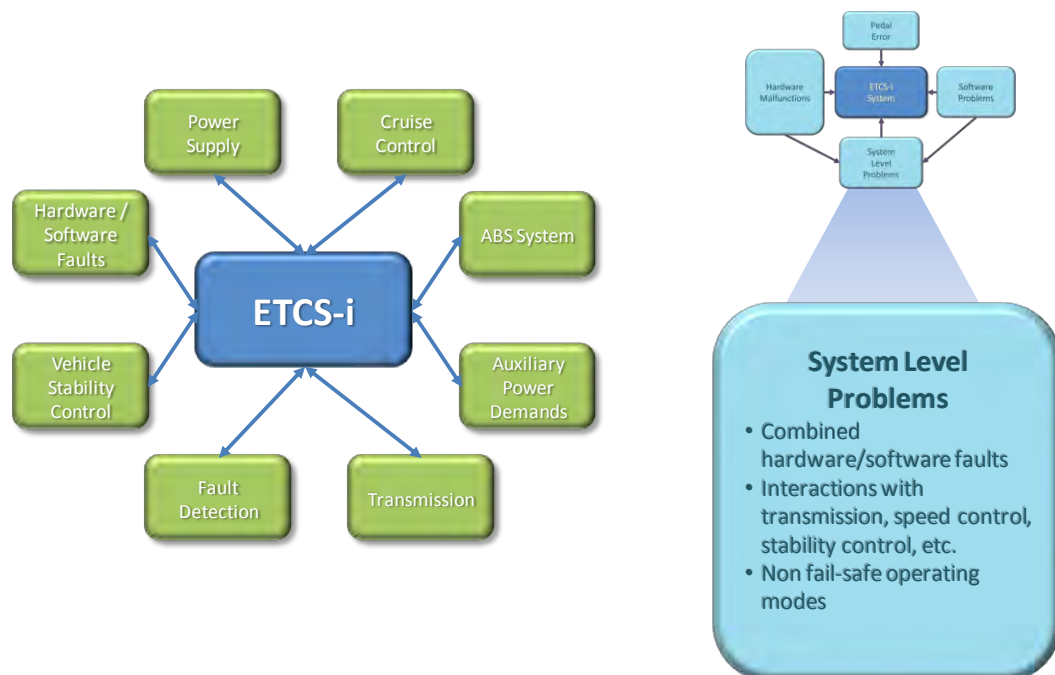


Figure 6. Subcategories of system level faults.

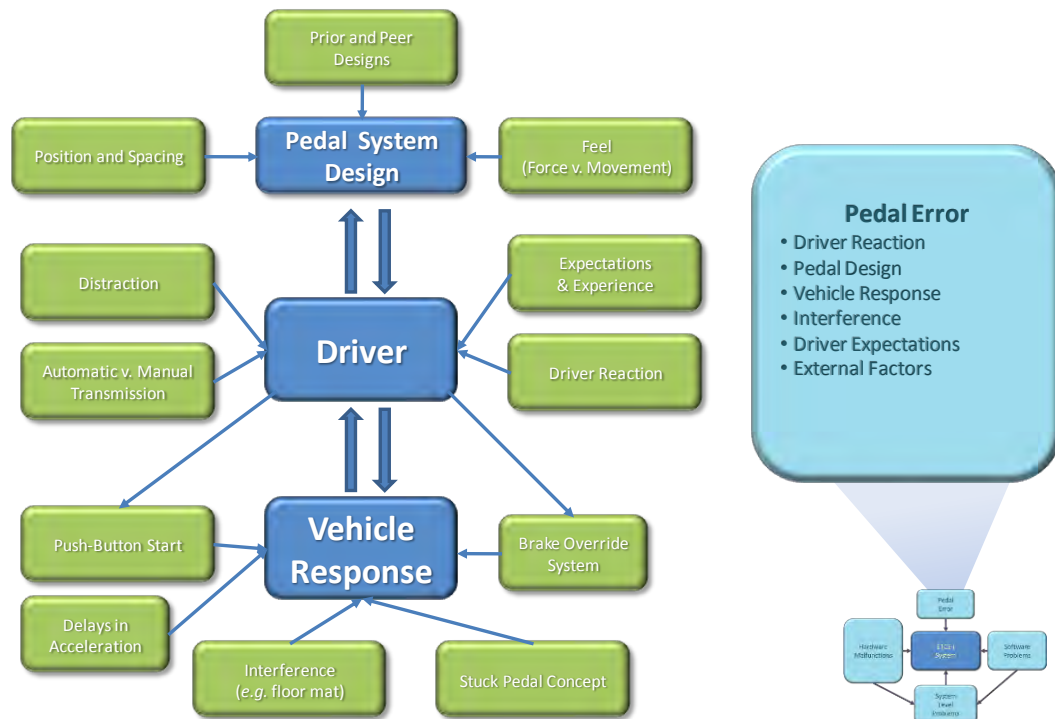


Figure 7. Subcategories of failures related to pedal error.

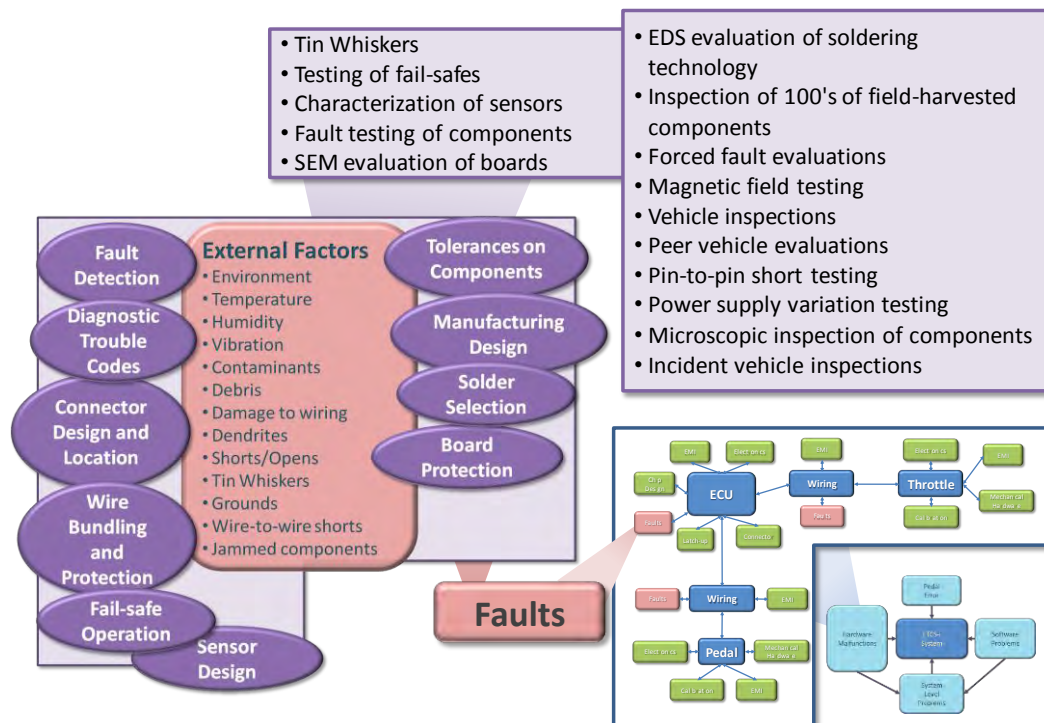


Figure 8. Details of some parts of the investigation associated with electrical faults.

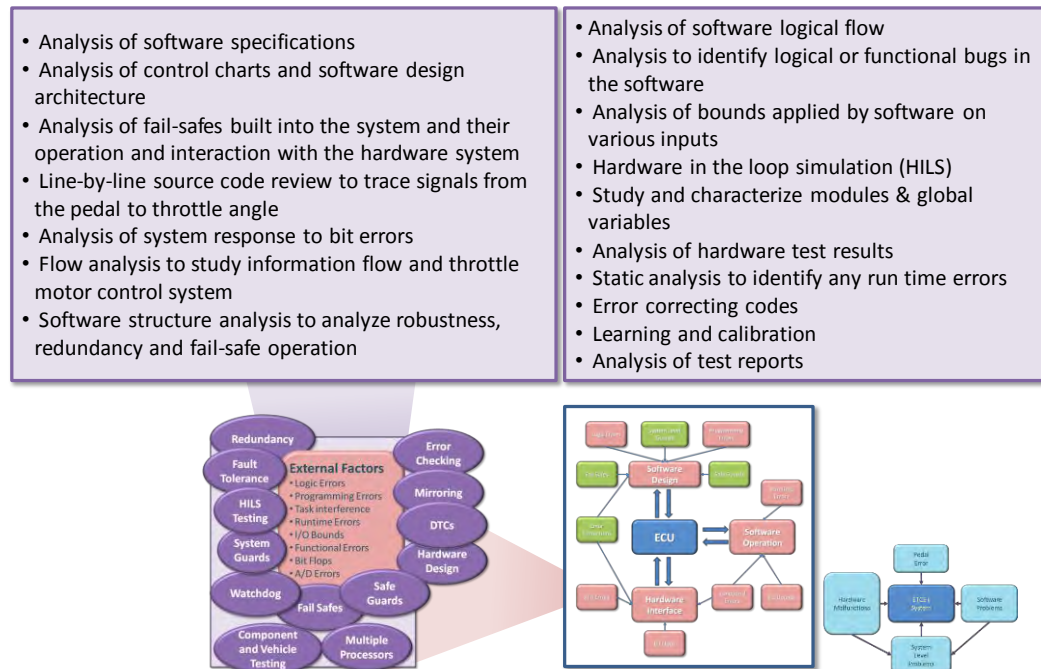


Figure 9. Details of some parts of the investigation associated with software faults.

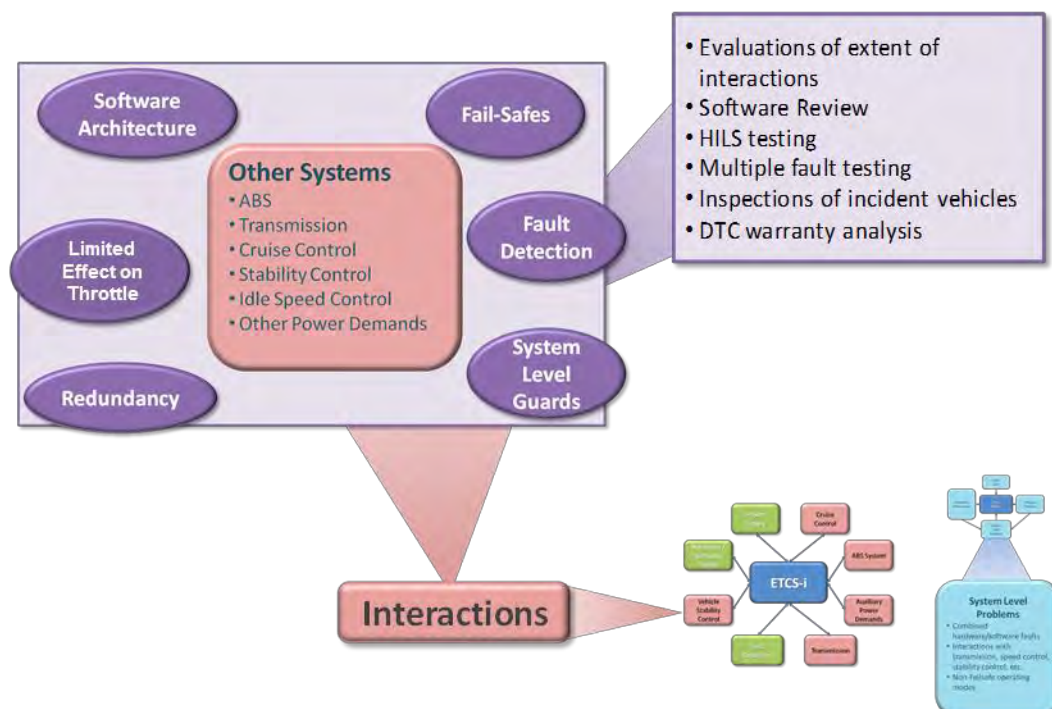


Figure 10. Partial investigation details associated with characterizing system level interactions.

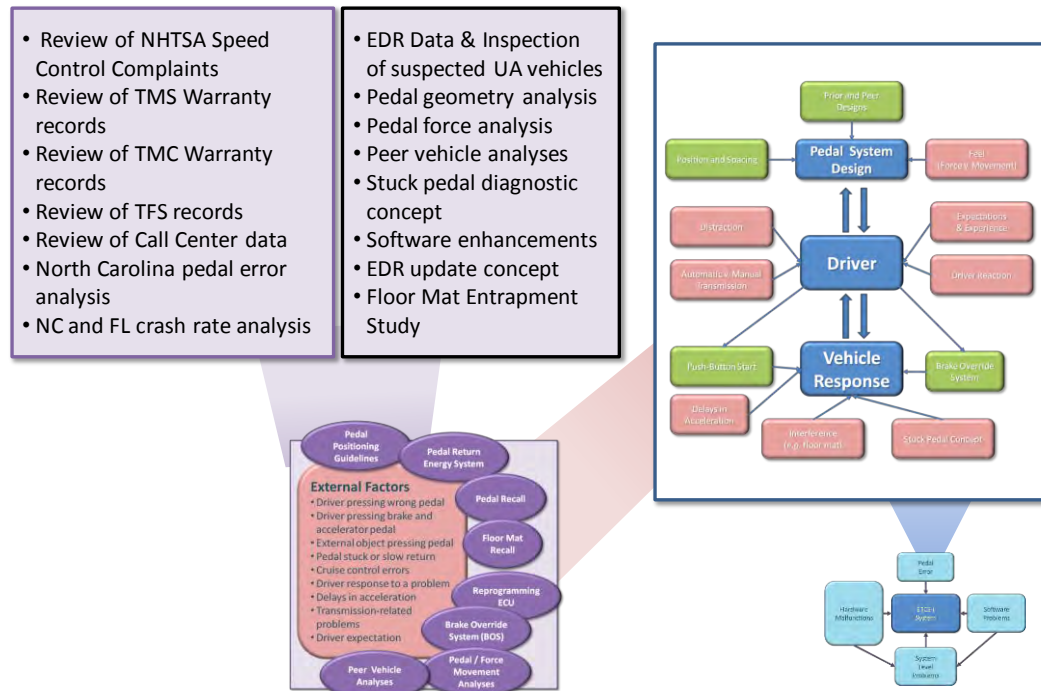


Figure 11. Partial investigation associated with pedal error.

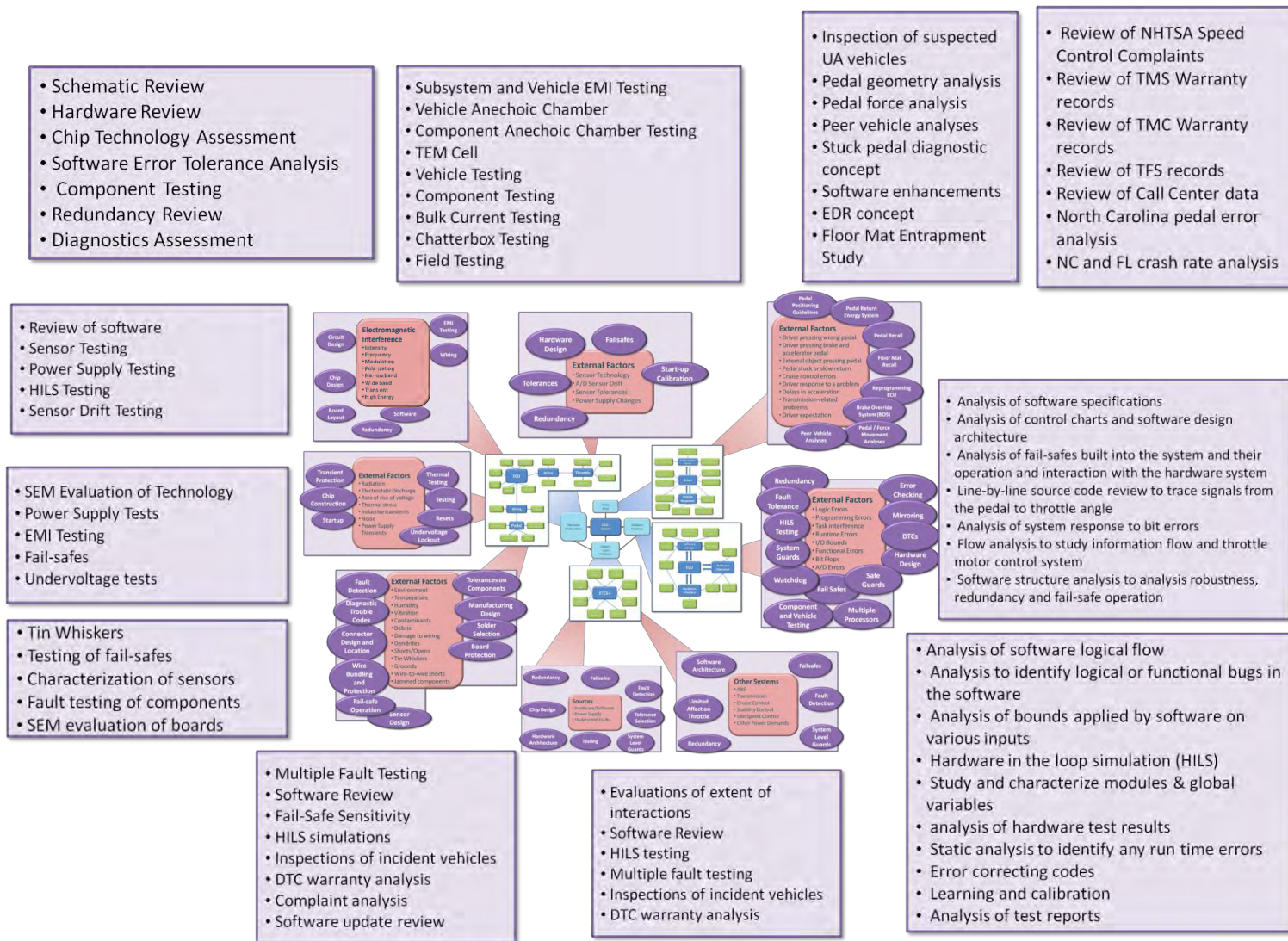


Figure 12. Investigation overview.

3 ETCS-i Basics and Operation

3.1 Introduction

As engine control technology has advanced and new sensors and technology have been introduced, the ECM has taken a progressively larger role in monitoring and control. Figure 13 shows the ETCS-i (Electronic Throttle Control System-intelligent) functional layout in Toyota and Lexus vehicles¹⁷. The accelerator pedal position is resolved by two sensors (with the outputs labeled VPA1 and VPA2) whose signals are transmitted to, and processed by the ECM. The ECM also receives signals from two throttle position sensors, VTA1 and VTA2. Based on these signals and inputs from other sensors, the ECM transmits a drive signal voltage to the throttle control motor to control the position of the throttle valve.

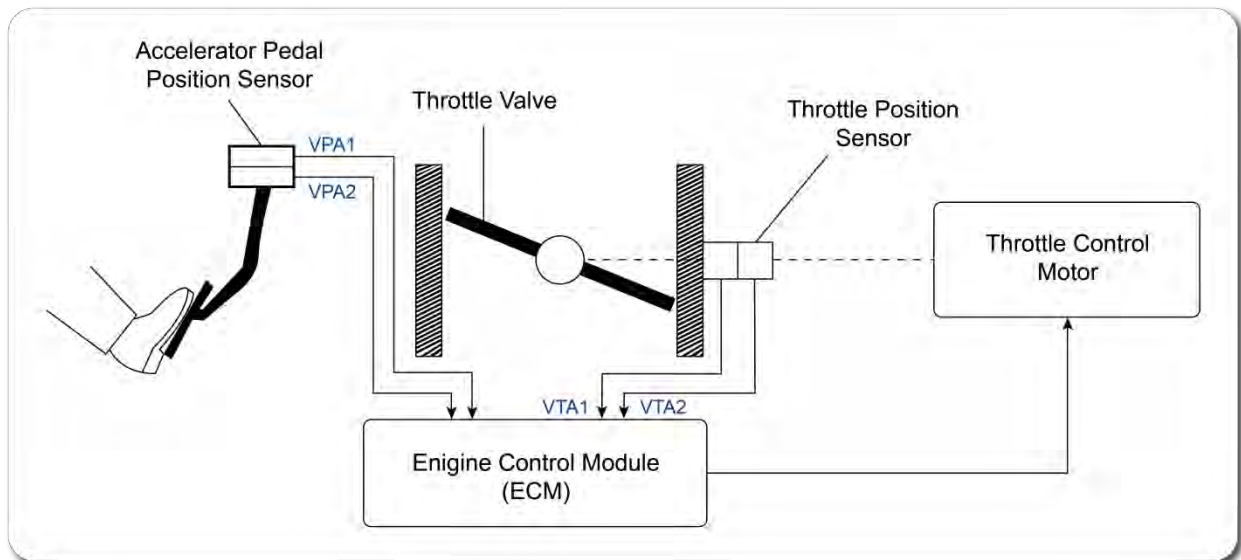


Figure 13. Electronic Throttle Control System with Intelligence Function Diagram.

¹⁷ This section uses material from Exponent's report, "Testing and Analysis of Toyota and Lexus Vehicles and Components for Concerns Related to Unintended Acceleration", February 2010.

3.2 Predecessor Cable System Design

Prior to the advent of the ETCS-i system, Toyota, like other manufacturers, had a mechanical linkage, such as a cable, connecting the accelerator pedal to the throttle valve on the throttle body. Figure 14 is a photograph of a pre-ETCS-i pedal and the cable that connects the pedal to the throttle valve.

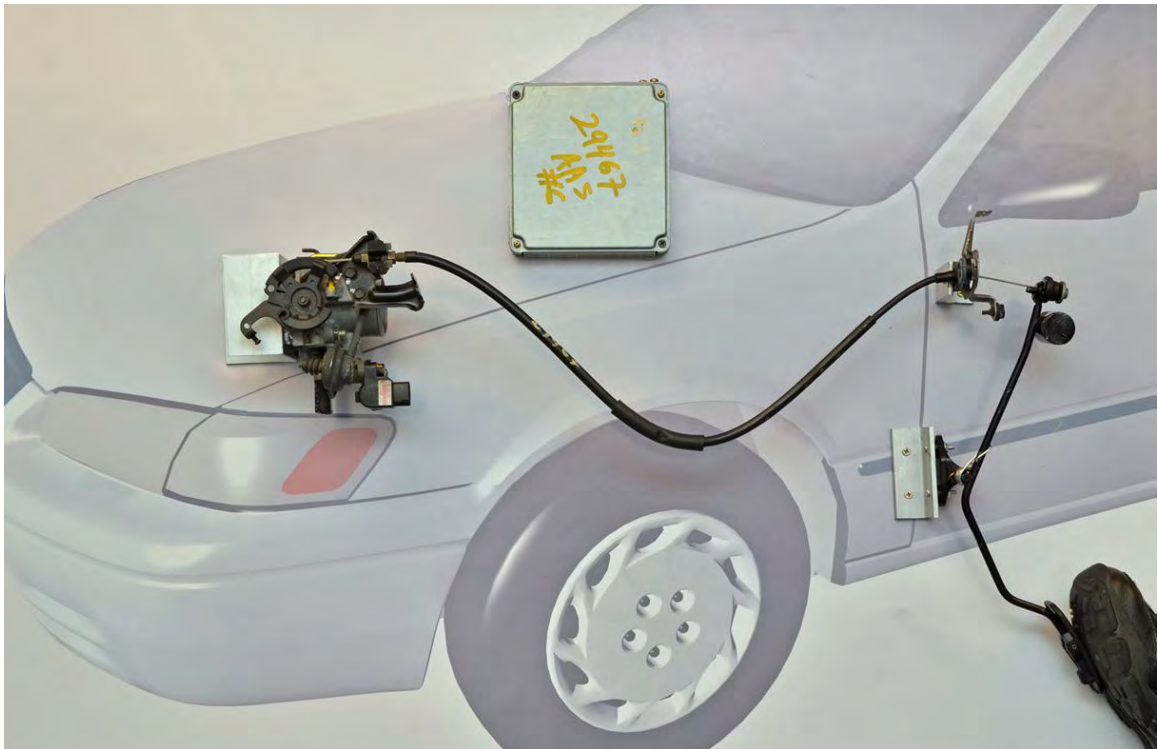


Figure 14. Cable-based throttle control design.

In this design, as the pedal is moved, the mechanical cable causes the throttle valve to open and close, controlling the volume of combustion air and thus the engine power. Figure 15 is an exploded view of a pre-ETCS-i throttle body using a mechanically actuated throttle valve. Note that this design also contains a throttle position sensor. The throttle position sensor (Figure 16) sends information regarding the throttle valve opening angle to the ECM, which uses this information and other data, to determine fuel injection, spark timing, and other parameters. The ECM in this older control design does not control the position of the throttle valve. Figure 17 shows a 1998 Camry L4 ECM (pre-ETCS-i).

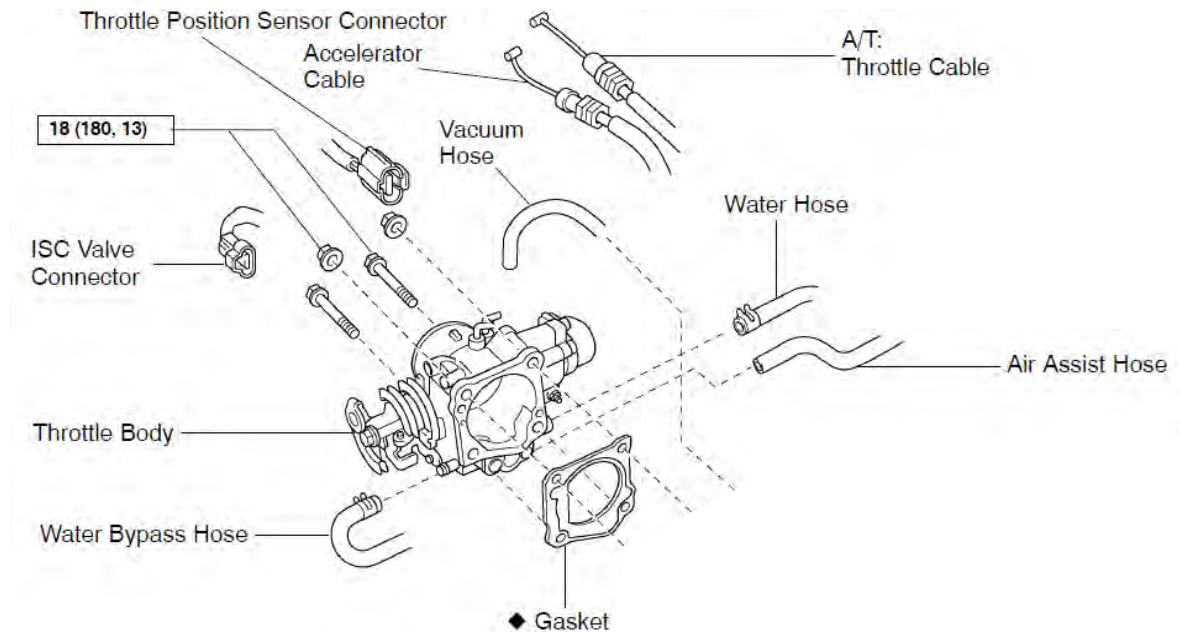


Figure 15. Pre-ETC throttle body system exploded view for a 2000 Tacoma L4 engine showing the accelerator cable and throttle position sensor connector.



Figure 16. 2004 Toyota Tacoma L4 pre-ETC throttle body mechanical linkage showing the accelerator pedal cable throttle valve control mechanism (white arrow) and the throttle position sensor (TPS – yellow arrow).



Figure 17. ECM from a 1998 Camry L4 (pre-ETCS-i).

3.3 ETCS-i

The development of the Electronic Throttle Control System with intelligence (ETCS-i) enabled better fuel economy, reduced emissions, certain stability control enhancements, and the implementation of hybrid engine technology, amongst other features.

The accelerator pedal in all Toyota vehicles equipped with ETCS-i technology has two position sensors that generate output voltages dependent on the pedal position. Figure 18 shows an accelerator pedal from an ETCS-i equipped 2009 Toyota Corolla. The throttle body also has dual throttle position sensors, each generating an output voltage proportional to the position of the throttle valve. Figure 19 shows the throttle body for a 2003 Toyota Camry. The ECM receives signals from the pedal position sensors and also from other sensors which it uses to calculate the desired throttle valve position. The ECM then controls the position of the throttle valve by controlling the current to the throttle motor. This control strategy results in a closed loop system, where the driver controls the vehicle speed or acceleration through the accelerator pedal or cruise control system, the ECM reads this input and uses feedback signals from a variety of sensors to calculate an appropriate throttle valve position, and then ensures that the throttle valve is at its commanded position. The ETCS-i also communicates with other electronic systems in the vehicle such as the vehicle stability control system and the electronic transmission system, and controls engine speed and torque accordingly.



Figure 18. Accelerator pedal for an ETCS-i equipped 2009 Toyota Corolla.



Figure 19. Throttle body from a 2003 Toyota Camry.

3.4 Fail-safes and Diagnostic Trouble Codes

Toyota vehicles set diagnostic trouble codes (DTCs) when a fault is detected in one or more sub-systems. The response of the vehicle to a DTC depends upon the type of fault that occurs and the classification of the fault in the software. Although the detection criteria and the circuits and conditions monitored are generally similar amongst the various Camry vehicles equipped with ETCS-i, changes have been made in the detection thresholds due to changes in hardware, software and/or regulatory requirements. The discussion in this document will use the 2007 Camry V6 as an example for illustration purposes. In the source code for the 2007 V6 Toyota Camry, fault conditions are classified into one of five categories:

- **Class 0:** Throttle control continues as normal. Malfunction indicator lamp (MIL) is not turned on.
- **Class 1:** Throttle control continues as normal. MIL is turned on.
- **Class 1.5:** Fail-safe throttle control. MIL is turned on.

- **Class 2:** Throttle motor system is shut down. Engine output is controlled by fuel injection (intermittent fuel-cut) and ignition timing to allow the vehicle to continue at a minimal speed. MIL is turned on.
- **Class 3:** Engine fuel is cut and the engine shuts down if air flow rises when this class of failure is triggered. MIL is turned on.

The vehicle continues to operate as normal and can be controlled and driven if a Class 0 or Class 1 fault is detected by the ECM.

Class 1.5 failures transition the vehicle into a fail-safe mode where the maximum speed at which the vehicle can be driven is limited. In addition, in this mode, pressing the brake pedal causes an immediate closing of the throttle valve. This mode of operation will also be referred to as the “limp-home” mode of operation.

Class 2 failures transition the vehicle into a fail-safe mode where the driver has limited ability to accelerate the vehicle. In this mode of operation, the power to the throttle motor is cut. The engine output is adjusted by the ECM by controlling the fuel injection and the ignition timing in response to the pedal depression. This mode of operation is referred to as the “fail-safe” mode of operation.

When in the Class 3 mode of operation, the vehicle’s engine shuts down if the air flow detected by the air flow sensor exceeds the air flow value calculated by the ECM.¹⁸

In addition to the fail-safe classes discussed above, the ETCS-i system is also designed with a fuel cut feature that monitors the engine rpm when the vehicle is at idle (i.e. the accelerator pedal is released). This feature stops the flow of fuel to the engine if the engine speed rises above 2500 rpm¹⁹ with the vehicle at idle.

¹⁸ And the engine rpm exceeds a minimal value.

¹⁹ This rpm value is vehicle specific.

3.5 Advantages of ETCS-i

Electronic throttle control represents an advancement in engine control technology enabling or facilitating new safety and performance attributes, including:

- Enabling additional safety features, such as vehicle stability control where the ECM reduces power transmission to the wheels to assist the driver in maintaining directional control
- Eliminating mechanical throttle cables and problems associated with these cable and throttle bodies, such as sticking
- Eliminating problems associated with prior technology such as idle air control hardware
- Adaptable throttle response to driver and driving conditions, such as snow mode (available on some vehicles) where the rate of throttle valve opening can be controlled to allow the reduction of engine output from normal
- Enabling greater throttle control under cold start and idle vehicle conditions or when coasting, reducing emissions and improving fuel economy
- Smoother shifting/transmission
- A simplified cruise control system, including the implementation of dynamic radar type cruise control
- Adaptation to changing engine loads from auxiliary equipment in the vehicle, for example, air conditioning etc.
- Enabling hybrid vehicle technology, such as when the vehicle is powered by electric motors, allowing the engine to autonomously turn on and off for improved fuel economy
- Increased flexibility for variations in vehicle features
- Improved self-diagnosis.

In summary, the multiple features and benefits of ETCS-i increase driver safety, improve emissions and fuel economy, and improve system reliability. Toyota and the rest of the automotive industry have shifted to the use of electronic based throttle control systems.

3.6 Camry ETCS-i technology

As discussed, the Camry was selected for a detailed study as part of this investigation. Electronic throttle control was introduced in the Camry starting with the 2002 model year. Other Toyota and Lexus models, including the 4Runner, Prius, Sequoia, Land Cruiser, Tundra, GS, IS, LS, LX and SC had various implementations of electronic throttle control systems in earlier model years than the Camry, extending back in some cases to the 1998 model year. Hardware design changes over the years are discussed further in Chapter 6. Other major changes in control hardware design/manufacturing for Toyota vehicles include:

- Lead (Pb) free solder was introduced starting with the 2008 Camry (both the L4 and V6 engine variants). This coincided with the introduction of nickel-palladium-gold coating for the pins of most ICs on the ECM.
- Conformal coating was used on ECMs for 2002 to 2006 model year Camry vehicles (both the L4 and V6 engine variants).
- The ECM was moved from the passenger compartment to the engine compartment starting with 2007 model year Camry vehicles (both the L4 and V6 engine variants). This coincided with the introduction of water-proof enclosures and connectors for the ECM.
- Transition to Hall Effect-based throttle position sensors starting with 2004 model year Camry (both the L4 and V6 engine variants). 2002 to 2003 model year Camrys utilized potentiometer throttle position sensors.
- Transition to Hall Effect-based accelerator pedal position sensors starting with the 2007 model Camry (both the L4 and V6 engine variants).

Accelerator pedal position sensors utilized potentiometers for the 2002 to 2006 model year Camry vehicles.

Software design changes have also occurred on electronic throttle control technology-equipped Camry vehicles (as well as on other Toyota and Lexus models) with the shift to a software architecture based on a powertrain manager configuration. Table 1 provides approximate transition model years for Toyota and Lexus vehicles to the power train manager-based architecture.

Table 1. Software architecture (throttle control system) design of Toyota and Lexus vehicles. (grey cells - power train manager based architecture)

Models		Calendar Year				
		2006	2007	2008	2009	2010
V6 (6AT)	Camry	Jan (07MY)				
	ES350	Jan (07MY)				
	Avalon			Aug (08MY)		
	Venza				Dec (09MY)	
	RX350				Jan (10MY)	
	Sienna					Dec (10MY)
V8 (6AT)	Tundra		Jan (08MY)			
	LC200			Oct (08MY)		
	Sequoia			Dec (08MY)		
	LX570			Nov (08MY)		
	GX460					Nov (10MY)
V8 (8AT)	LS460		Sep (07MY)			
	GS460			Oct (08MY)		
	IS-F			Dec (08MY)		

Software diagnostics have also changed for ETCS-i technology-equipped Camry vehicles in response to:

- Change in the SAE diagnostic code requirements
- Change in the high level hardware design (e.g. change in the number of ECM processors)
- A change in the diagnostic module specifications (for example due to updated requirements from the California Air Resources Board (CARB)). These changes will be discussed in detail in other sections of the report.

4 Accelerator Pedal

Exponent's analyses and investigations into the design and performance characteristics of accelerator pedals used on Toyota vehicles equipped with ETCS-i technology in this chapter will encompass:

- The operation of the accelerator pedals
- The interaction of the accelerator pedal signals with the ETCS-i system
- Potential failure modes of the pedal's electrical circuit (pedal circuit)
- Response of the vehicle to multiple failures on the pedal circuit.

The testing detailed in this chapter is not inclusive of all pedal tests performed. The testing discussion will focus on pedal operation and system failure response.

4.1 Introduction

This chapter addresses the response of the ETCS-i system to accelerator pedal failure modes. ETCS-i technology uses electrical circuits in the pedal assembly to measure the pedal depression and transmit this information to the ECM, unlike earlier "drive-by-cable" vehicles where the accelerator pedal was connected mechanically to the throttle valve. The ECM processes the pedal information to determine the air quantity to the combustion chamber via the appropriate throttle valve angle. The driver provides input via the driver-controlled movement of the accelerator pedal to communicate the desired speed to the ECM. The ETCS-i uses a closed-loop control throttle valve system to ensure that its actual position matches the desired position, based on driver's input and engine operating conditions.

With ETCS-i technology, accelerator pedal assembly sensors generate dc voltage signals proportional to the pedal position. The pedal circuit failures that were evaluated and discussed in this report include:

- Sensor failure modes
 - Open-circuit failure
 - Short-circuit failure
 - Latch-up
- Calibration drifts
- Electrical noise²⁰ (circuit design)
- Resistive faults
- Power supply variations.

Testing and analyses of the various pedal circuits were performed to characterize and determine the response of the pedal circuits to various induced faults or abnormal operational conditions. The remainder of this chapter will describe the pedal circuit and its operation, and, summarize the testing and analysis performed.

4.2 Pedal Circuit and Operation

In ETCS-i technology, two pedal assembly electrical circuits measure pedal depression and transmit proportional voltages to the ECM, called VPA1²¹ and VPA2.²² VPA1 provides the position of the pedal and VPA2 is used to monitor and verify VPA1. Toyota vehicles equipped with ETCS-i technology have used two different sensor technologies: potentiometer-based and Hall Effect sensor based.

²⁰ The EMI testing performed is discussed in a separate Exponent report.

²¹ In some manuals, VPA1 is sometimes referred to as VPA.

²² The first generation of ETCS-i systems had the accelerator pedal position sensors mounted on the throttle body and connected to the pedal by a cable. These sensors had two outputs, VPA1 and VPA2, but shared a common voltage supply and ground circuit.

4.2.1 Potentiometer based Pedals

Potentiometer based accelerator pedals contain two potentiometers that measure the pedal position and communicate this information to the ECM. Two different manufacturers (Aisan and Denso) provided the potentiometer based pedals used in Toyota models. While the physical designs of the two pedals are different, the electrical circuit characteristics are similar. Figure 20 shows an Aisan potentiometer-based pedal used on a 2002 Camry, and Figure 21 shows its internal electrical construction.



Figure 20. Aisan potentiometer pedal.

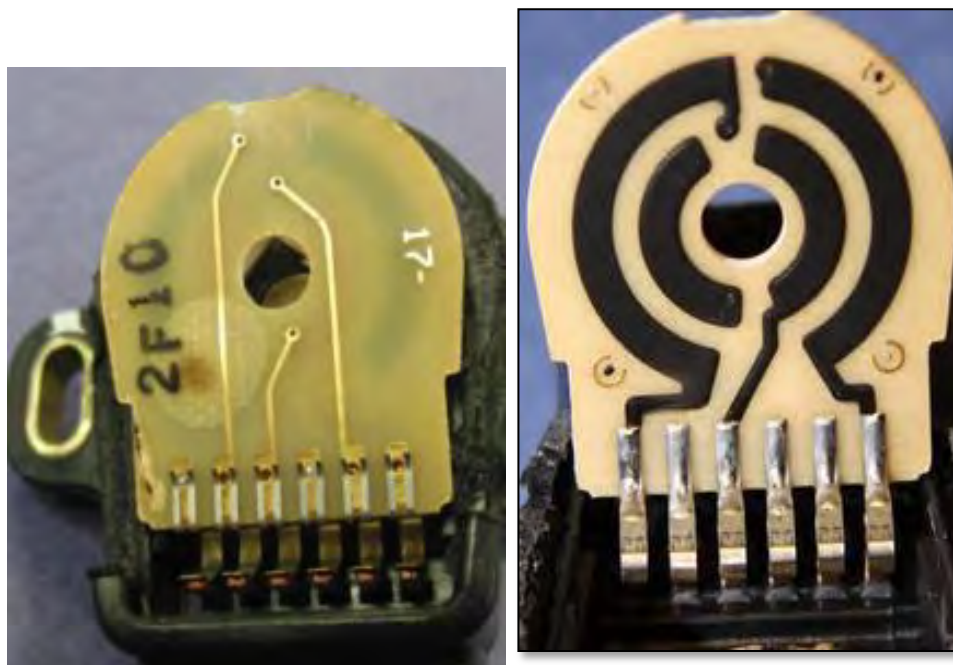


Figure 21. Aisan potentiometer pedal sensor.

Figure 22 shows the internal construction of the potentiometer-based pedal manufactured by Denso. This pedal design does not utilize a solder connection between the pedal electrical circuit and the pedal connector. Instead, a physical contact is made to complete the electrical connection between the pedal connector and the pedal circuit.



Figure 22. Denso potentiometer based pedal sensor.

Since the Denso and Aisan potentiometer pedal electrical circuits are similar, the discussion in the remainder of this chapter will focus on the Aisan potentiometer pedal by way of example. The potentiometers are used in voltage divider circuits. The outer and inner rings on the circuit serve as the resistive elements and the means for conveying the output voltage to the connector. The rotating arms (wipers) support the contacts that connect the outer and inner rings. During pedal depression, the contacts of the potentiometers slide along the resistive elements, changing the values of the resistances in the two voltage divider circuits. These changes in resistance cause corresponding changes in the output voltage signals generated by the potentiometer. Thus, the outputs from the two potentiometer circuits, VPA1 and VPA2, change with the position of the pedal. The voltage offset between VPA1 and VPA2 is set by the relative wiper positions along the potentiometers' circumferences. The potentiometer circuit output voltage signals are transmitted to the ECM where they are filtered and processed.

The two potentiometer based circuits have the following characteristics:

- Over the nominal operating range the VPA2 signal has a positive voltage offset of approximately 0.8 Vdc compared with the VPA1 signal
- With pedal depression and angle increase, both signal voltages increase in a parallel linear fashion
- For a pedal in the “released” position (at idle), $VPA1 \approx 0.8$ and $VPA2 \approx 1.6$ V
- The maximum voltages occur with the pedal fully depressed as discussed in section 4.2

Figure 23 is a plot of the VPA1 and VPA2 signals as a function of the rotation of the pedal sensor for a 2002 V6 Camry. Note that the x-axis represents the change in angle of the sensor contacts along the contact surface and not the change in angle of the pedal arm.

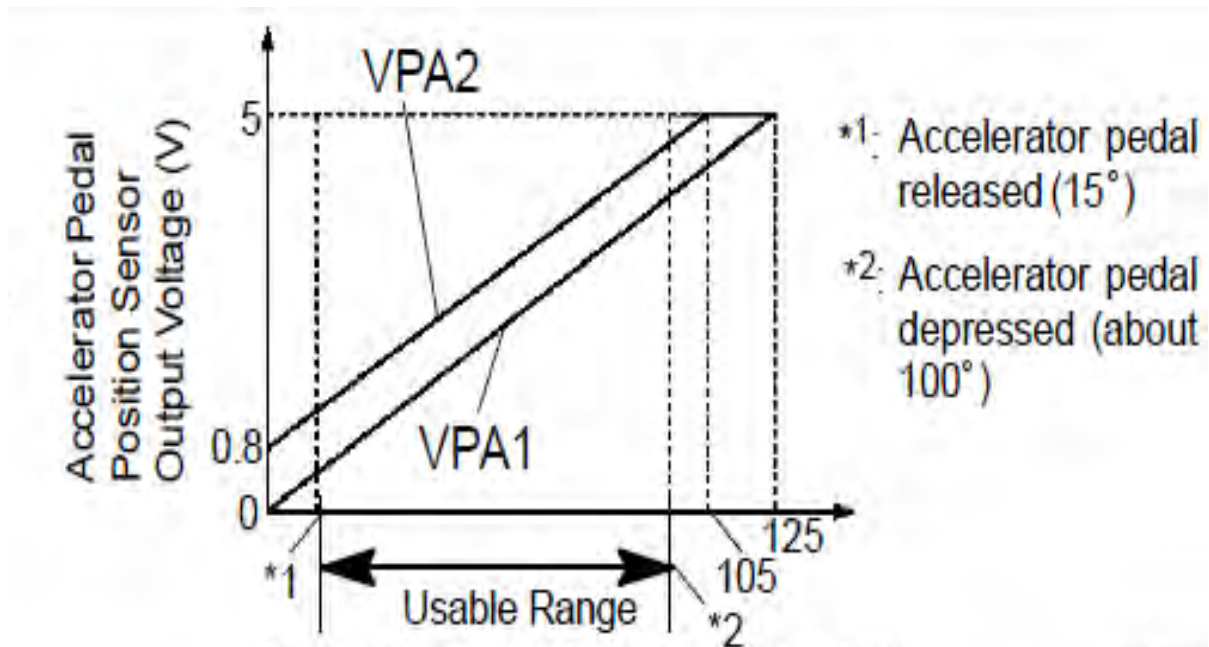


Figure 23. Nominal voltage outputs for a potentiometer-based pedal sensor as a function of rotation of the pedal sensor.

The angular range through which the potentiometer-based sensor rotates from idle to full throttle is greater than the angular range over which the pedal itself travels. This arises from the geometry of the pivot axes for the pedal and pedal sensors, as shown in Figure 24. This arrangement provides a greater usable arc on the sensor resistive elements, which is advantageous for purposes of durability and sensitivity.

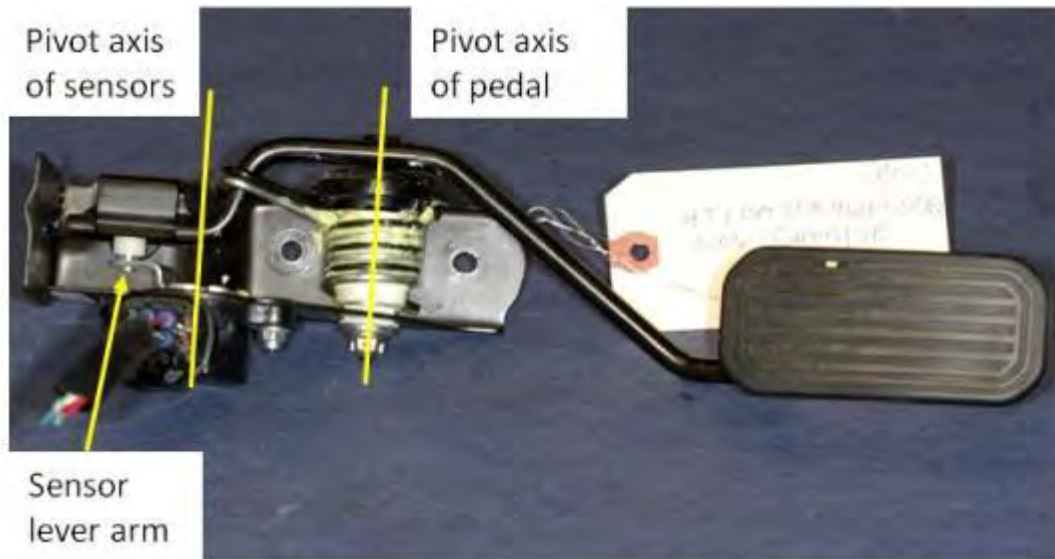


Figure 24. Potentiometer pedal geometry (2006 Camry V6).

4.2.2 Hall Effect sensor based pedals

A different sensor technology is used in Hall Effect sensor-based pedals for measuring the accelerator pedal position. A Hall Effect sensor is a transducer where the output voltage varies in response to a magnetic field. Accelerator pedals equipped with Hall Effect sensors rely on two Hall Effect sensors to detect the position of the pedal and communicate this information to the ECM. When the pedal is depressed, powerful rare earth permanent magnets move relative to the sensors, producing a change in the normal component of the magnetic field strength detected by the sensors. The strength of the normal component of the magnetic field is related to the position of the pedal. The Hall Effect sensors detect the magnetic field strength and generate output signals VPA1 and VPA2 in response. Unlike the potentiometer-based sensors, the Hall Effect sensors do not have a moving contact, so contact wear is eliminated.

The output signals from Hall Effect sensor-based pedals (similar to potentiometer pedals) have the following characteristics:

- As the pedal is depressed and pedal angle increases, both signal voltages increase in a parallel linear fashion

- For a released pedal (at idle), $VPA1 \approx 0.80 \text{ V}$ and $VPA2 \approx 1.60 \text{ V}$
- Over the nominal operating range, VPA2 has a positive voltage offset of approximately 0.8 Vdc as compared with VPA1, i.e. $VPA2 \approx VPA1 + 0.8 \text{ V}$
- A specified operating temperature range of $\blacksquare^\circ\text{C}$ to $\blacksquare^\circ\text{C}$ and a storage temperature range of $\blacksquare^\circ\text{C}$ to $\blacksquare^\circ\text{C}$.

Figure 25 is a block diagram of the Hall Effect sensor-based pedal and the pedal circuit output voltage characteristics with pedal depression.

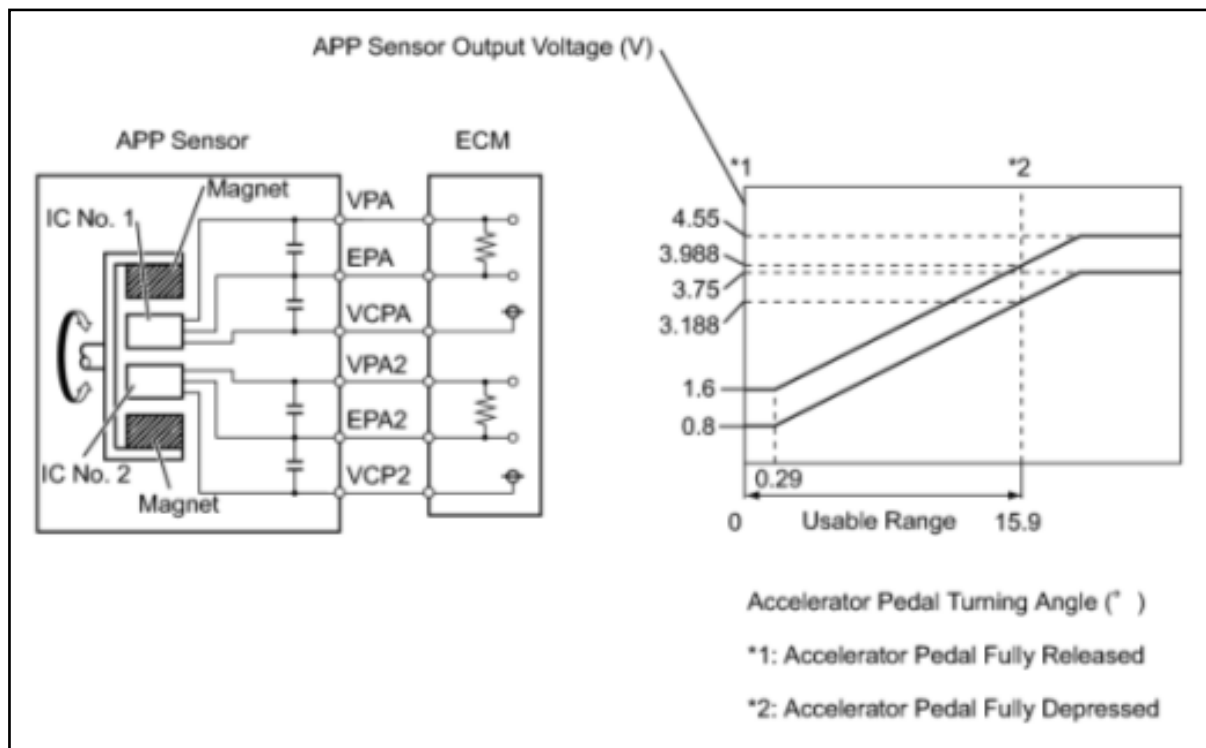


Figure 25. Hall Effect sensor output characteristics.

Toyota Hall Effect sensor-based pedals utilize two distinct designs and are sourced from two manufacturers. These are:

- CTS Hall Effect sensor based pedals (CTS pedals)
- Denso Hall Effect sensor based pedals (Denso pedals).

4.2.2.1 CTS Hall Effect Based Pedals

Figure 26 and Figure 27 show the electrical circuit board of a CTS Hall Effect based pedal (CTS pedal). In this pedal design, the two independent Hall Effect sensors and their associated signal processing circuitry are included in a single IC. The IC has a power supply pin, ground pin, and single output pin for each sensor. Though the two sensors reside on the same IC, they do not have any electrical interconnections on the IC. The two sensors have independent power supply and ground traces, except for a high-frequency common-mode capacitor between the two ground terminals.

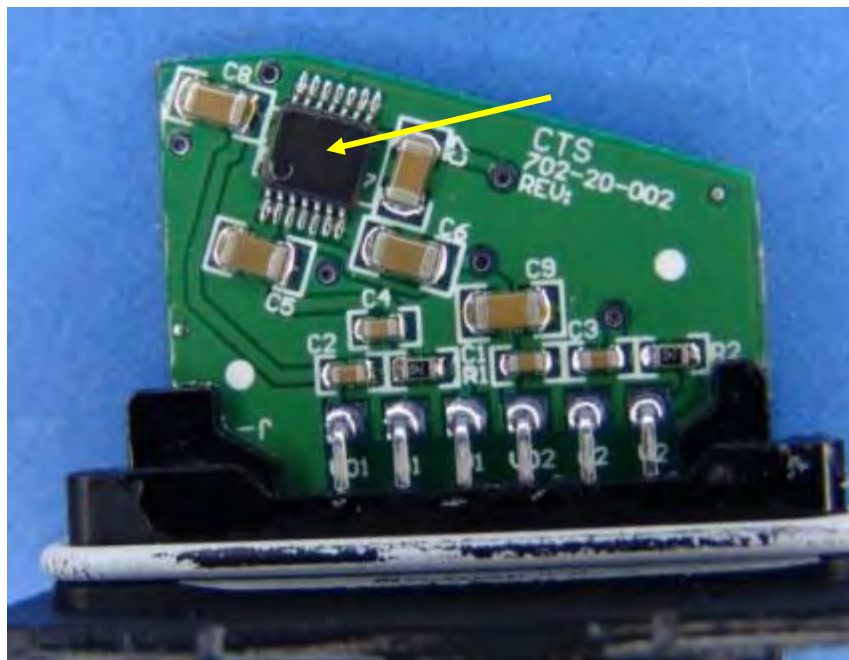


Figure 26. The Hall Effect sensor IC (yellow arrow) on a CTS pedal circuit containing the two independent Hall Effect sensors, and the resistors and the capacitors used for filtering and decoupling.

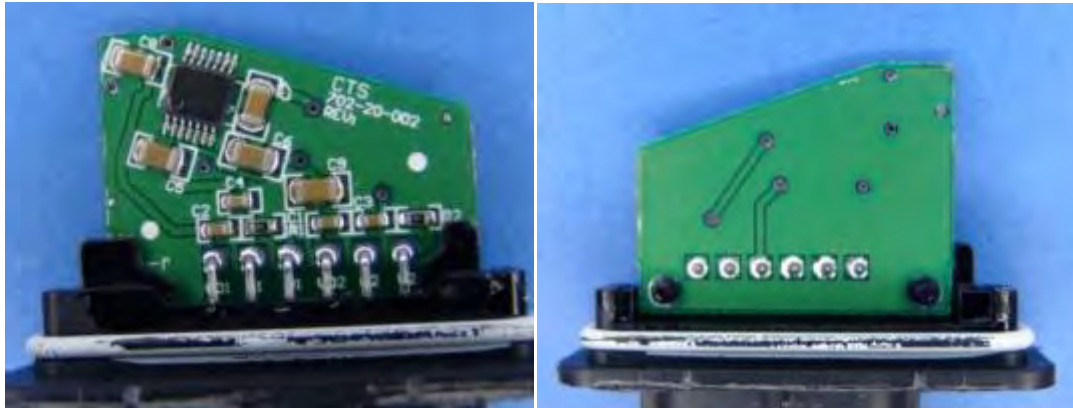


Figure 27. Top and bottom surfaces of the CTS circuit board.

4.2.2.2 Denso Hall Effect Based Pedals

Figure 28 shows the Denso Hall Effect sensor-based pedal internal construction, and Figure 29 is a pedal circuit x-ray image. The Denso pedal circuit contains two independent Hall Effect sensor ICs with filter capacitors at each of the power supply terminals and at each of the output terminals. These filter capacitors enhance and improve immunity to electrical noise.

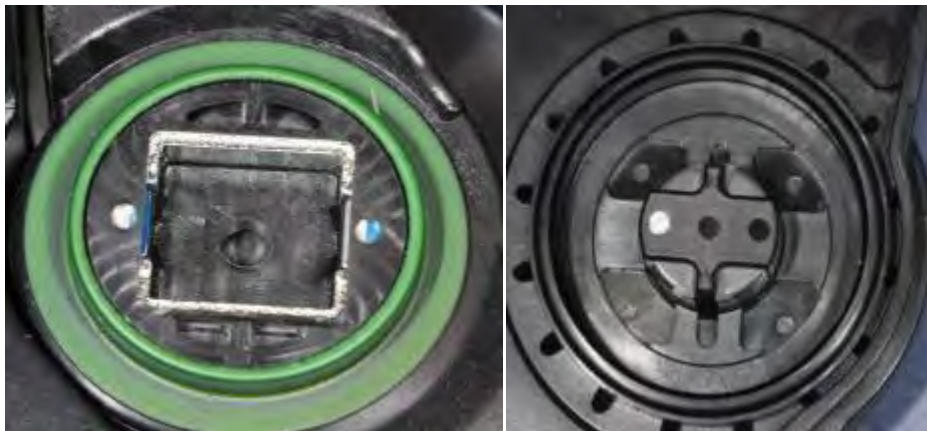


Figure 28. Denso pedal permanent magnets (left) and Hall Effect sensors (right).

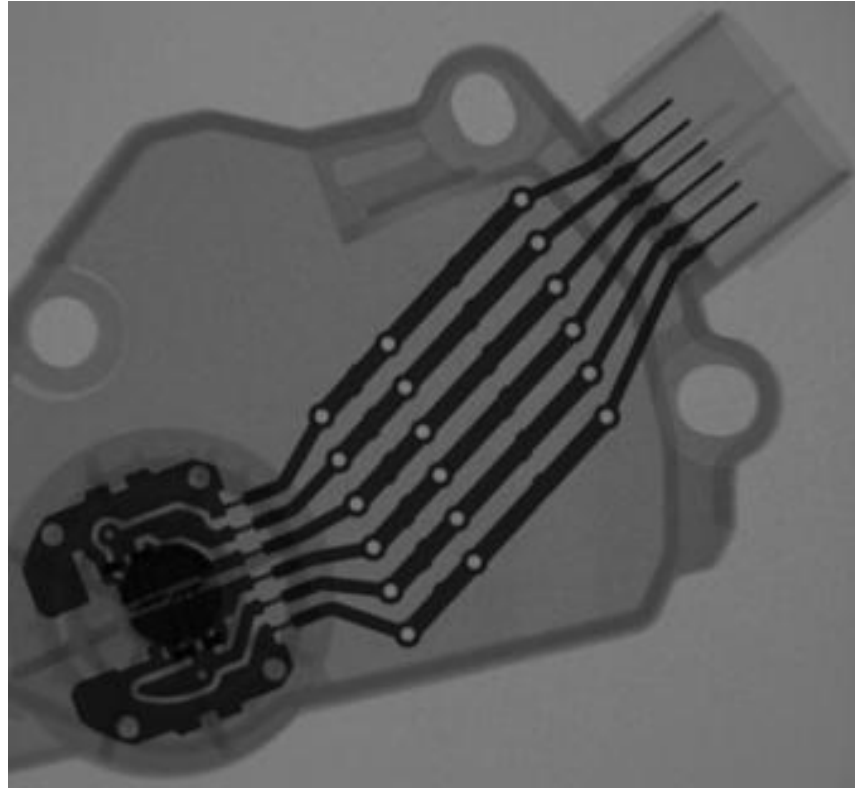


Figure 29. X-ray image of Denso Pedal circuitry showing the two Hall Effect sensors and the electrical traces. Each Hall Effect sensor has a power supply and output terminal filter capacitor.

4.2.3 Characterization Tests

Accelerator pedal output voltages as a function of pedal depression were characterized to quantify the operation of the pedal circuits. Figure 30 illustrates the voltage outputs, VPA1 and VPA2, as a function of pedal displacement angle, for eight different Toyota and Lexus accelerator pedals.

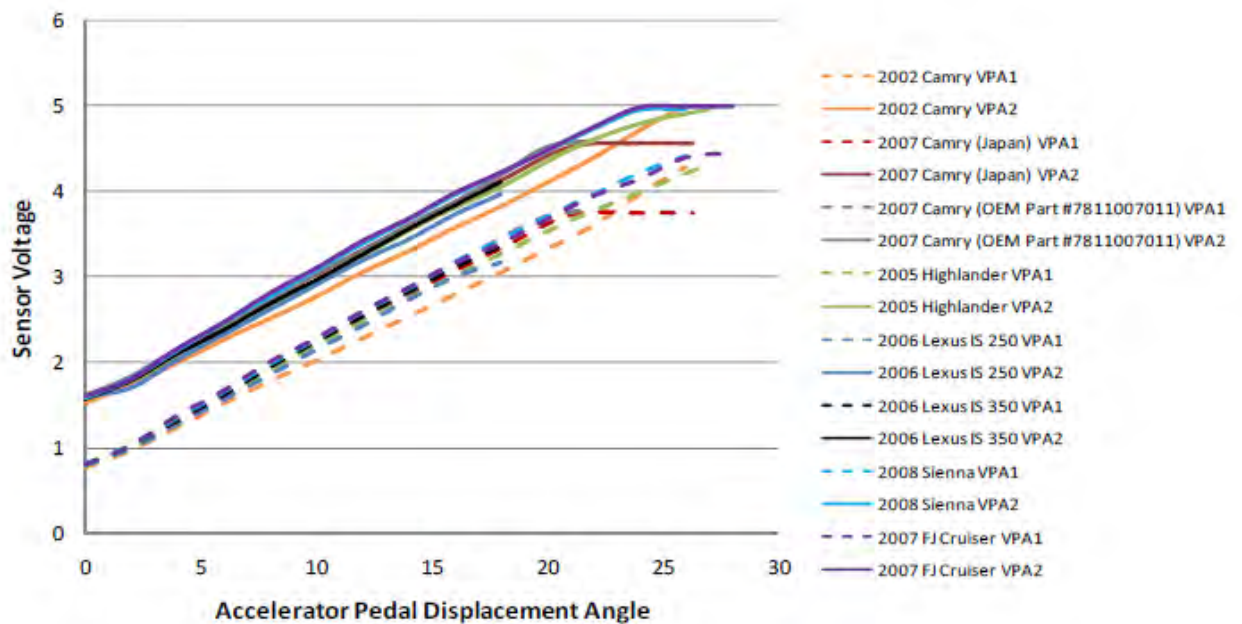


Figure 30. Accelerator pedal sensor voltages as a function of pedal angle for selected Toyota and Lexus pedals.

4.3 Pedal Interaction with ETCS-i system

Two circuits in the pedal assembly detect the pedal position and produce the two proportional output voltages VPA1 and VPA2 for the ECM to determine pedal depression. When the vehicle is at idle, VPA1 and VPA2 have a positive offset of 0.8 V and 1.6 V respectively, relative to ground. The two signals increase in a parallel fashion as a function of accelerator pedal rotational angle (Figure 31) for a Hall Effect sensor.

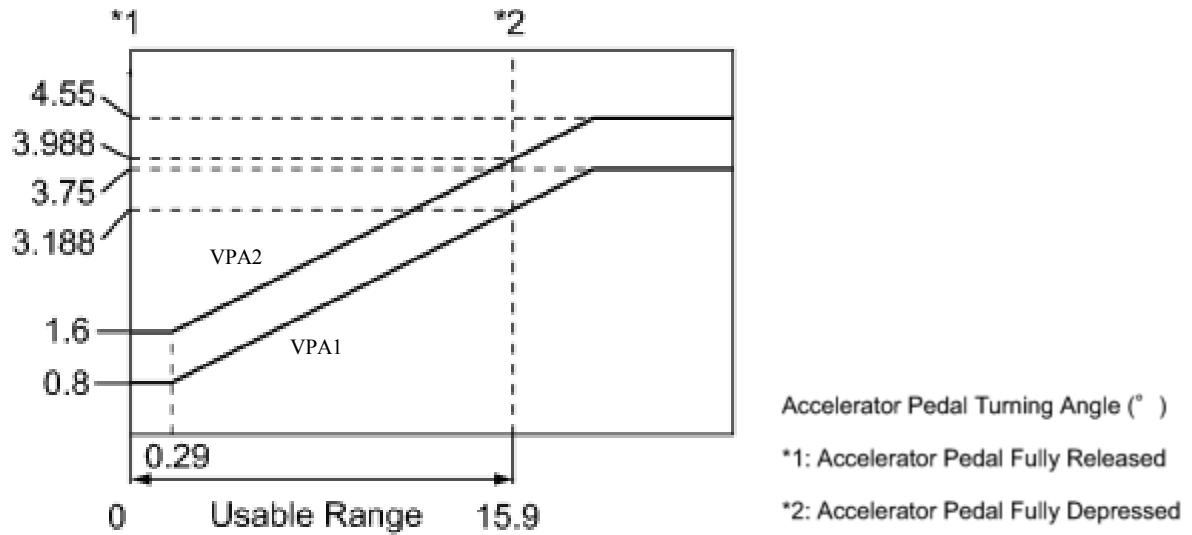


Figure 31. Hall Effect pedal sensor output as a function of accelerator pedal turning angle.

The ECM uses the VPA1 signal to determine the actual pedal displacement angle and for engine control. The VPA2 signal is used as a functional check on the accelerator pedal position sensor output, VPA1.

A parallel voltage profile with position for the pedal outputs as compared to non-parallel/diverging signals (i.e. signals with different gradients) has certain advantages for accelerator pedal position sensing. These include:

- Wider Monitoring Range:** The use of parallel slopes for the sensor output signals can provide a wider monitoring range because with diverging signals, the signal with the steeper gradient can reach the upper limit sooner, creating a region where the relationship between VPA1 and VPA2 cannot be monitored with precision. This concept is illustrated in Figure 32 below.

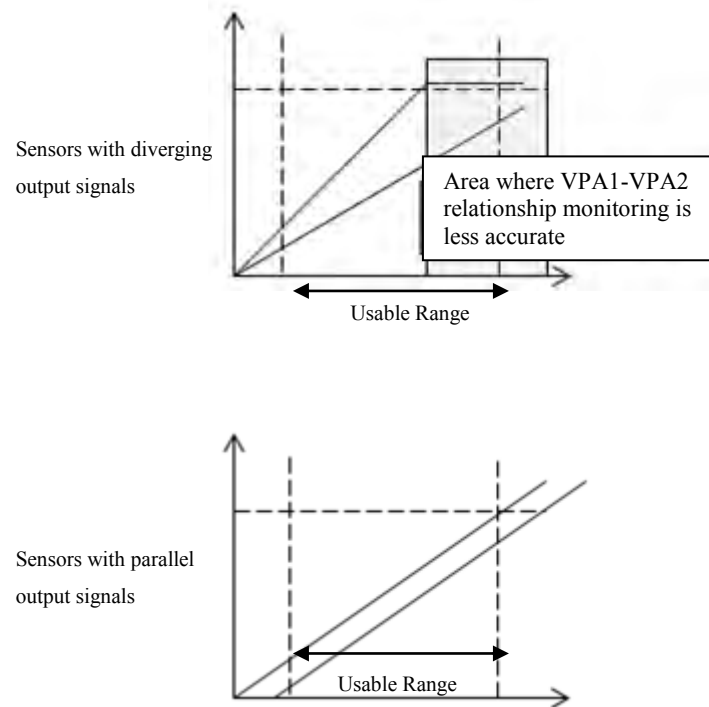


Figure 32. Monitoring range and accuracy for pedals with parallel and diverging outputs.

- Higher Resolution:** The ECM uses the voltage of the VPA1 signal to determine the driver input and correspondingly activate the throttle motor. The use of diverging signals limits the signal resolution and accuracy by limiting the voltage range of the signal with a lower gradient as illustrated in Figure 33. The reduction in the accuracy results in a larger throttle opening angle variation for small changes in VPA1.

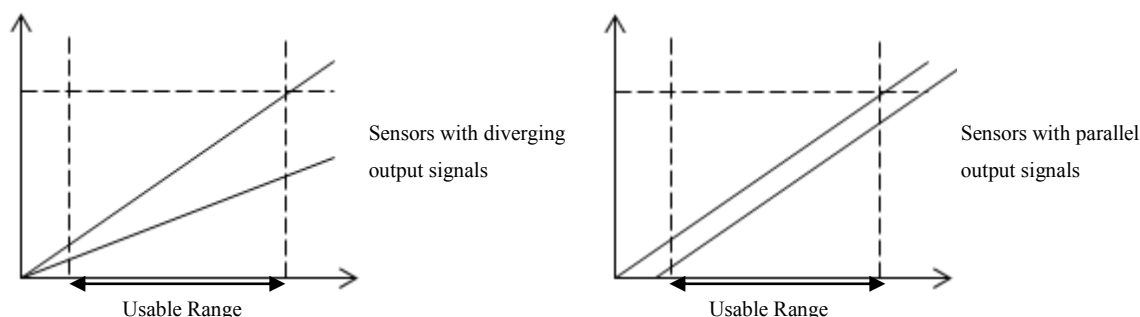


Figure 33. Signals with parallel slopes provide increased resolution by using a larger voltage range for the same pedal angle range.

4.4 Accelerator Pedal Fail-safes

The ECM monitors the pedal position sensors and sets a DTC if the sensor outputs are outside a pre-set range, indicating that there is a fault in the accelerator pedal circuit. Fault conditions such as an open-circuit fault or a short-circuit fault may cause the pedal output signals to deviate from their expected values. Pedal specific DTCs in Camry vehicles are summarized in Table 2. DTC fault conditions in other Camry model year vehicles are almost identical, the slight deviations being due to requirements mandated by the California Air Resources Board (CARB).

Table 2. DTC associated with pedal faults

DTC 2003–2009 Camry	DTC 2002 Camry	Description ²³	Fault Condition
P2120	P1120	Throttle/Pedal Position Sensor D Circuit	VPA1 Intermittent Open/Short
P2122	P1120	Throttle/Pedal Position Sensor D Circuit Low	VPA1 Open, Ground Short
P2123	P1120	Throttle/Pedal Position Sensor D Circuit High	VPA1 short to high
P2125	P1120	Throttle/Pedal Position Sensor E Circuit	VPA2 Intermittent Open/Short
P2127	P1120	Throttle/Pedal Position Sensor E Circuit Low	VPA2 Open, Ground Short
P2128	P1120	Throttle/Pedal Position Sensor E Circuit High	VPA2 short to high
P2138	P1120	Throttle/Pedal Position Sensor D/E Correlation	Lose Pedal Connector, VPA1 and VPA2 dead short
P2121	P1121	Throttle/Pedal Position Sensor D Range/Performance	Rationality between VPA1 and VPA2

²³ The description of the DTC on the table is for the 2003 – 2009 Camry.

The fault detection scheme for the pedal monitors the VPA1 and VPA2 signals to ensure that they are within an acceptable range.²⁴ Figure 34 shows the allowable values for VPA1 and VPA2 for a 2007 V6 Camry.²⁵ Figure 35 illustrates the combinations of VPA1 and VPA2 which trigger DTCs.

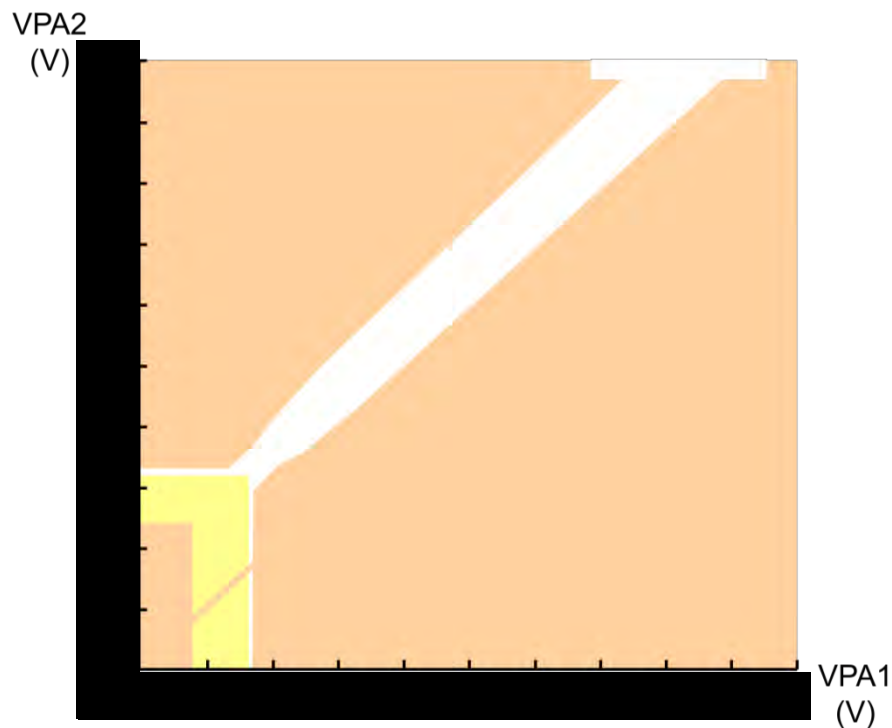


Figure 34. Allowable values for VPA1 and VPA2.²⁶

²⁴ Faults are triggered if the absolute values of the output of the two independent pedal circuits fall outside the acceptable values or if the relationship between the two pedal circuit output signals deviates from the designed relationship

²⁵ This range applies to a condition after the pedal position learning at ignition on has been completed

²⁶ Nominally VPA1 and VPA2 will be 0.8 V and 1.6 V respectively at idle. The two signals increment in a parallel fashion with the VPA2 at a positive offset (of 0.8 V) with respect to VPA1. Hence, the combination of VPA1 and VPA2 signal in the yellow zone should not occur in a normal working pedal. If the pedal output signals fall in this area, the vehicle would decelerate regardless of driver request. VPA1 and VPA2 in the orange zone will trigger a DTC and transition the vehicle to the “limp-home” mode

In addition to monitoring the absolute values of the VPA1 and VPA2 signals, the relative values of the VPA1 and VPA2 signals are also monitored. A DTC is set if:

- The difference between the two pedal output signals is too small or too large
- Either of the two pedal output signals deviates from their allowed values under normal operating conditions.

The allowable deviation is dependent upon the pedal turning angle and is the smallest when the vehicle is at idle (i.e. no pedal depression).

4.5 Pedal Position Learning and Related Vehicle Operating Modes

The nominal values of VPA1 and VPA2 under idle conditions (0.8 V and 1.6 V) increase with pedal angle and follow the direction of the green arrow shown in Figure 35. However, to account for pedal position sensor “drift”, a pedal position “learning” (calibration) process occurs each time the ignition is turned on. This learning process determines the “new” pedal position sensor output signal values at idle to correct for any small variations in the pedal position sensor output values over the life of the vehicle.²⁷

Once the pedal position learning is performed, the range of allowable values for VPA1 and VPA2 are restricted; a deviation from the allowable values triggers a DTC and transitions the vehicle to the limp home mode (see section 4.4).

4.5.1 Narrow Lane

The amount of deviation allowed in the values of the VPA1 and VPA2 signals from their nominal values is restricted, limiting the range of allowable values for VPA1 and VPA2 (Figure 35). A small deviation from the normal relationship as shown by the white space around the

²⁷ Appendix B lists conditions that may cause the values learned for diagnostics to be updated during vehicle operation.

green arrow in Figure 35 is permitted to account for small variations in the potentiometer/Hall Effect sensor output voltages over the life of the vehicle. This allowable deviation results in a narrow band of allowable values for the VPA1 and VPA2 signals as depicted in Figure 35.

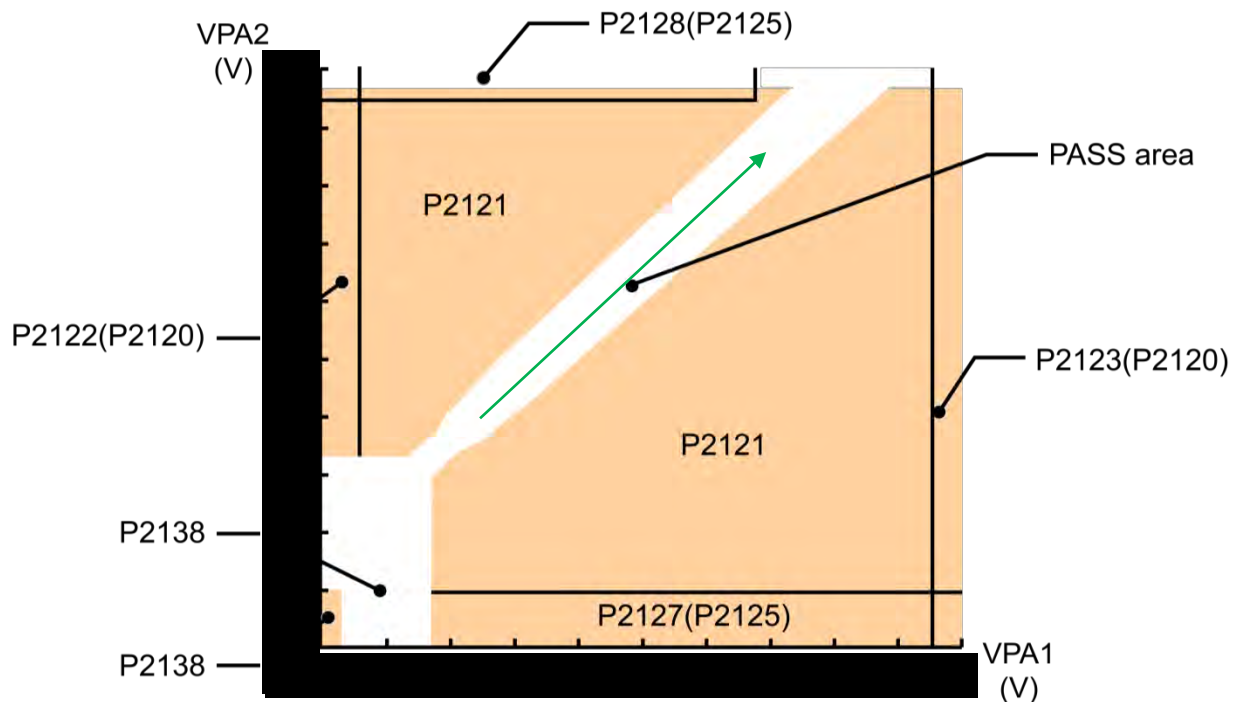


Figure 35. Allowable values for VPA1 and VPA2 (2003 - 2005 Camry).

If a fault occurs such that the values of the VPA1 and VPA2 signals fall outside this “narrow” band of operation, a DTC is triggered and the vehicle transitions to the limp-home mode. The DTC triggered depends upon the values of VPA1 and/or VPA2 (see Figure 35). The occurrence of a fault and the triggering of the DTC code results in the vehicle transitioning to a limp-home mode. In this mode:

- The vehicle operates in the power limit mode (i.e. maximum throttle opening is limited)
- In this mode, the throttle closes to the spring-controlled default position when the brake is pressed.

4.5.2 Wide Region

The learning process may not occur at ignition ‘on’ under certain conditions. If the learning process does not occur, the pedal position sensor values ‘learned’ during the last ignition on/off cycle are used (if available). If there is no history of pedal position learning (e.g. the vehicle’s battery is replaced, causing a loss of all information stored in memory), and if pedal position learning is not performed at ignition on (e.g. the ignition is turned on with the pedal depressed), the default idle values for VPA1 (0.8 V) and VPA2 (1.6 V) are used. In addition, the allowable deviation in VPA1 and VPA2 is extended (Figure 36) to a “wider” region of operation. As with the operation in the ‘narrow’ region, a DTC is triggered if VPA1 and VPA2 fall outside the now wide region of operation and the vehicle transitions to the limp-home mode. In this mode, depressing the brake pedal causes the throttle request from the pedal to return to 0°, regardless of the pedal request.

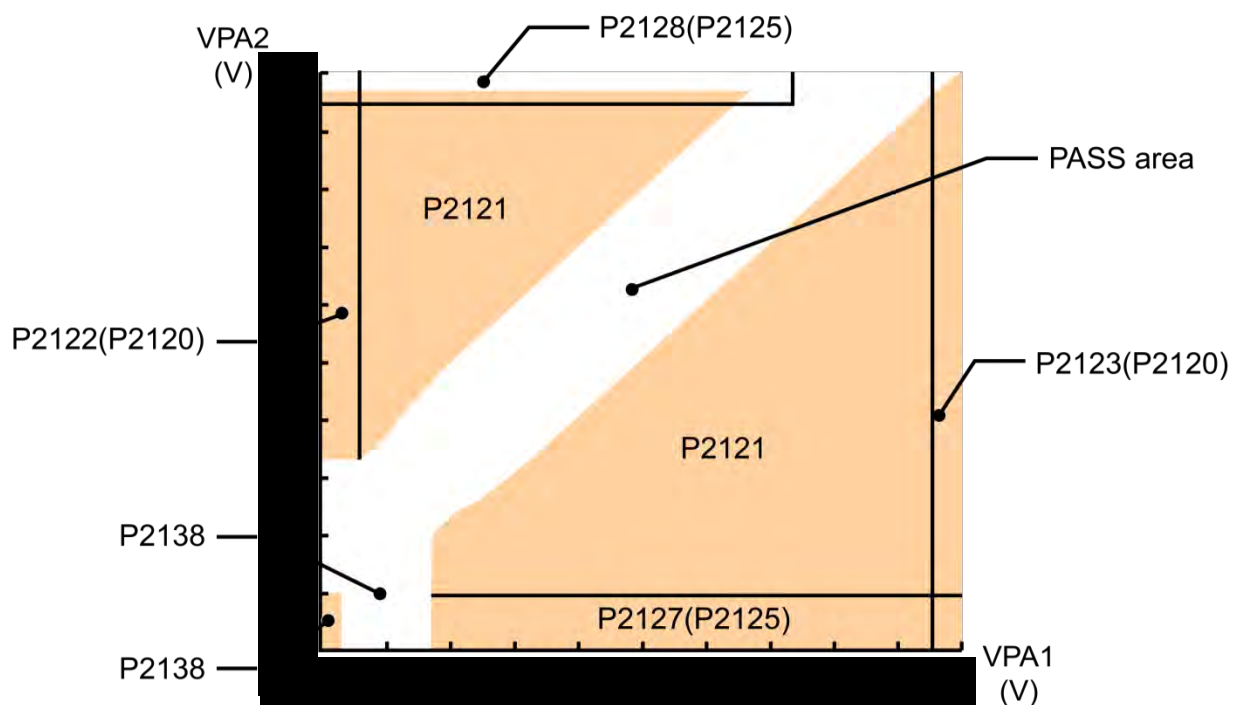


Figure 36. Allowable VPA1 and VPA2 (2003 - 2005 Camry) with no pedal position learning at ignition on and no pedal position learning history.

4.6 Pedal Circuit Failure Modes

This section will discuss the following topics related to the pedal circuit:

1. Sensor failures
2. Calibration
3. Electrical noise²⁸ (circuit design)
4. Resistive faults
5. Power supply variations.

One representative of the many variations in pedal circuit and Toyota ECM designs will be discussed. Response of the system to a failure may depend on components external to the accelerator pedal. This section will cover the response of the ETCS-i system to accelerator pedal circuitry failures.

4.6.1 Sensor Failures

The ETCS-i system detects short-circuits, open-circuits and pedal sensor output signal disagreements. These failures cause the ECM to set a DTC and transition the vehicle to the limp-home mode of operation (see section 4.4). A latch-up of the Hall Effect sensors would cause excessive pedal output signal deviation, which would trigger a DTC and transition the vehicle to the limp-home mode. Table 6 summarizes the various possible pedal circuit latch-up scenarios.

²⁸ The EMI testing that was performed is discussed in a separate Exponent report.

Table 3. Vehicle response to a latch-up of the Hall Effect sensors in the pedal circuit

Circuit	Circuit Condition due to Latch-up	Vehicle Response
VPA1 ²⁹	High	If VPA1 rises to the power supply voltage (+5 Vdc), DTC P2123 triggers; transitioning the vehicle to the limp-home mode.
	Low	If VPA1 drops to ground, DTC P2122 triggers, transitioning the vehicle to the limp-home mode.
		If VPA1 changes such that neither DTC P2122 nor DTC P2123 are triggered, DTC P2121 is triggered if the difference between the VPA1 and VPA2 exceeds the allowable range.
		If VPA1 latches up but a DTC is not triggered, one of the following will occur: If the engine is at idle, it will remain at idle (as the VPA2 idle flag remains unchanged). The latched-up value for VPA1 will be "learned" as the new idle value. If the vehicle is being driven, it may either accelerate or decelerate depending upon the value of VPA1. If the driver releases the pedal, VPA2 signal will return to the idle value while VPA1 signal will remain latched-up. This will trigger DTC P2121. If the driver continues to press the accelerator pedal after VPA1 latches-up, the vehicle may accelerate or decelerate depending upon the value of the VPA1 signal after latch-up.
VPA2 ³⁰	High	If VPA2 rises to the power supply voltage (+5 Vdc), DTC P2128 triggers transitioning the vehicle to the limp-home mode.
	Low	If VPA2 drops to ground, DTC P2127 triggers, transitioning the vehicle to the limp-home mode.
	Intermediate	If VPA2 changes such that the neither DTC P2127 nor DTC P2128 are triggered, DTC P2121 which monitors the relationship between VPA1 and VPA2 will be triggered if the difference between VPA1 and VPA2 exceeds the allowable range. VPA2 is used to monitor the circuit that generates VPA1. Hence, a VPA2 latch-up condition that does not trigger a DTC will not affect the throttle opening angle and the vehicle will continue to operate normally.
VPA1 & VPA2		If both sensors latch-up and rise to the power supply voltage or drop to ground, numerous DTCs (as discussed above) will be triggered transitioning the vehicle to the limp-home mode. Based on the analysis above, latch-up conditions affecting both the VPA1 and VPA2 values at the same time and resulting in acceleration without triggering any DTCs or activating any limp-home mechanisms are not realistic and are not consistent with the reported incidents of unintended acceleration.

²⁹ If the VPA1 latch-up does not affect its value, then the vehicle operates normally.

³⁰ If the latch-up condition does not affect the value of the VPA2 signal, then the vehicle will continue to operate normally.

4.6.2 Calibration

The Hall Effect ICs compensate for temperature induced variations. In addition, the software system is designed to constantly monitor the pedal position sensor outputs and trigger a DTC if the values are outside certain thresholds. If the sensor outputs deviate a small amount from their designed/expected values, the system is designed to account for this deviation. If this deviation exceeds certain thresholds, the system will set a DTC and transition the vehicle to the Class 1.5 limp-home mode (see section 3.4).

4.6.3 Electrical Noise

Electromagnetic interference, transients etc. can potentially interfere with the circuitry in the pedal and cause deviant outputs. Several design features incorporated into the pedal circuits and the ECM provide protection against electrical noise. EMI testing was performed by Exponent to identify whether the ETCS-i circuit was susceptible to electrical noise that could lead to UA. The EMI testing, which is detailed in a separate Exponent report³¹, did not identify any susceptibility of the vehicles to EMI that could explain reported incidents of unintended acceleration.

4.6.3.1 Potentiometer Pedals

The electrical circuits on Aisan and Denso pedals contain purely passive resistive elements. There are no circuit components to couple electrical noise onto the pedal signals to the ECM and affect the operation of the potentiometer pedal circuits. Electrical noise that may be coupled to the potentiometer pedal output signals would be filtered by the ECM pi-filter network and pull-down resistor. In addition, potentiometer-based pedals are not susceptible to latch-up. During extremely high level noise immunity testing (orders of magnitude higher than ambient levels) noise that was coupled directly into the wiring thermally damaged some of the potentiometer pedal sensor elements (see Figure 37) and caused the vehicle to transition to a Class 1.5 limp-home mode of operation. The damage caused by this testing was permanent,

³¹ Exponent report: "Evaluation of the Effects of Electromagnetic Fields on the Behavior of Electronic Throttle Control Technology Used in Toyota Vehicles,"

detected by sensor testing, and would be readily apparent upon examination of the sensor. If the output lead loses electrical connection to the potentiometer, the ECM pull-down resistor will pull the voltage low, triggering a DTC and transitioning the vehicle to the Class 1.5 limp-home operation.

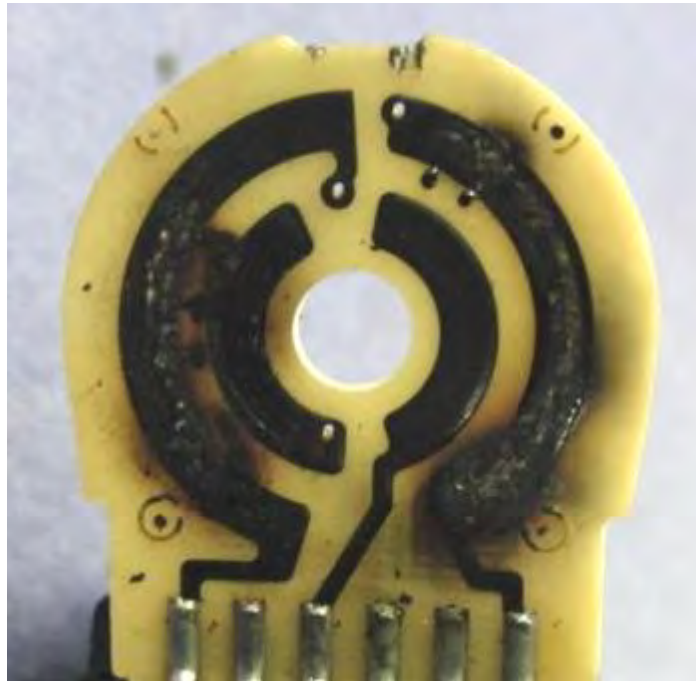


Figure 37. 2004 Camry pedal position sensor after the injection of high current RF at EPA wire.

4.6.3.2 Hall Effect CTS Pedals

The CTS pedal electrical circuit includes several elements to mitigate electrical noise interference. These include:

- Discrete resistors and capacitors that provide independent passive low pass filtering for the Hall Effect sensor dc power supply
- Filter capacitors at the output voltage terminals for EMI and ESD noise immunity and protection.

4.6.3.3 Hall Effect Denso Pedals

The Denso pedal electrical circuit includes several elements for noise immunity. These include:

- Independent passive low pass filtering external capacitors for the dc power supply used to power each Hall Effect sensor
- Filter capacitors at the output voltage terminals for EMI and ESD noise immunity and protection.

4.6.4 Resistive Faults and Contaminant Intrusion

Contaminants and/or tin whiskers (Appendix G) can lead to a resistive fault between the various signals in the pedal circuits. Several pedal design features provide protection against contaminants.

Potentiometer Pedal — The individual passive resistive elements in the potentiometer pedal circuit have relatively large creepage paths between them. In addition, there are no active components on the circuit. Furthermore, the pedal housing is enclosed, providing protection against moisture intrusion and other contaminants. The potentiometer circuit is positioned vertically above and away from the pedal foot pad, and potential damage. The six-pin pedal connector has rubber gaskets to prevent contaminant intrusion and make the connector waterproof (Chapter 11). Should contaminant intrusion occur, evidence and signs of resulting parasitic resistive electrical connection(s) would remain. No such evidence of contaminant intrusion has been found to date. Turning the car “off” and then “on” would not eliminate such fault evidence.

CTS Pedals — CTS pedals contain a circuit board sealed with a protective conformal coating that guards against moisture intrusion and other contaminants. Figure 38 shows the pliable rubber gasket on the waterproof connector rim. Electronic modules can develop parasitic resistive connections over time and fail³² due to contaminants from manufacturing or

³² “Tutorial, Failure-Mechanisms for Conductive-Filament Formation”, IEEE Transactions on Reliability, Vol. 43, No. 3, September, 1994.

contaminant intrusion. Contamination intrusion leaves visual evidence, and no such evidence of contaminant intrusion has been found to date. Turning the car “off” and then “on” would not eliminate such a fault.

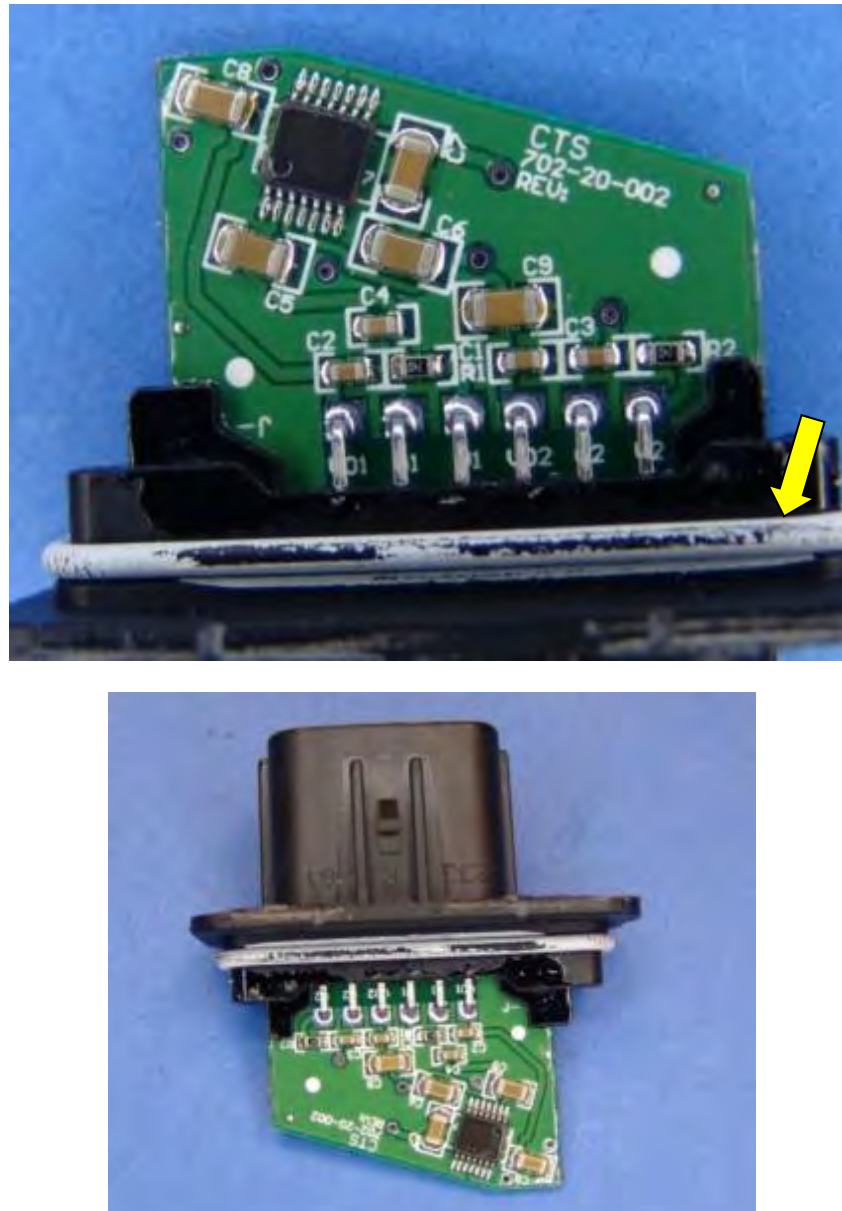


Figure 38. CTS pedal circuit board. Arrow shows the pliable rubber gasket surrounding the rim providing a waterproof seal.

Denso Pedal—The electrical circuit on the Denso pedal (which includes the ICs and the filter capacitors) is potted. This seals the circuit, protecting it against the intrusion of moisture and other contaminants. This sealing mechanism provides effective protection against the

introduction of contaminants and prevents resistive faults on the pedal circuit. Should the potting be damaged and contaminant intrusion occur, the unmistakable evidence would remain. No such evidence has been found to date. The connector is sealed by a pliable waterproof rubber gasket to prevent contaminant intrusion.

4.6.4.1 Tin Whiskers

Tin whiskers may induce shorting by direct bridging and contact between adjacent conductors; breaking off one component and shorting two nodes elsewhere on the board (for unpotted and uncoated boards); and electro-magnetic radiation emission.³³ Whisker formation requires tin plated electronic components but can be mitigated by a variety of means.³⁴ Whiskers exhibit variable incubation periods and growth rates, but grow monotonically and tend to asymptotically reach maximum lengths.^{35,36} Growth rate and maximum length depend on materials, environment, and countermeasures.^{37,38}

Accelerator pedal sensors from model years 2002 to 2009 were inspected in accordance with National Aeronautics and Space Administration (NASA) and industry guidelines using both optical and scanning electron microscopy. Board solders, solderability platings and component plating composition were determined using energy dispersive spectroscopy. Conformal coatings were analyzed with optical microscopy for thickness and Fourier-transform infrared spectroscopy for composition. Tin whisker susceptibility varies across Toyota's accelerator pedal electronics and sensor types:

-
- ³³ J. Smetana and R. Gedney, "Tin whisker management guidelines, part 2," <http://pcdandf.com/cms/magazine/172/2278-tin-whisker-management-guidelines-part-2>; this analysis indicates that EMI may be an issue for communication speeds above 6 GHz, which are well above those employed in Toyota engine control, accelerator pedal, and throttle body electronics.
- ³⁴ iNEMI, "Recommendations on lead-free finishes for components used in high reliability products," Version 4, December 2006, http://thor.inemi.org/webdownload/projects/ese/tin_whiskers/Pb-Free_Finishes_v4.pdf
- ³⁵ S. Sakuyama and M. Kutami, "Substitute materials for complete elimination of hazardous substances – study of whisker growth on lead-free plating," *Fujitsu Science and Technology Journal*, 2005, **41**(2), pp. 217-224.
- ³⁶ M. Dittes, P. Oberndorff, and L. Petit, "Tin whisker formation – results, test methods, and countermeasures," *Proceedings of the 53rd Electronic Component and Technology Conference*, 2003, pp. 822-826.
- ³⁷ J. Smetana, "Theory of tin whisker growth – the end game," *IEEE Transactions on Electronic Packaging Manufacturing*, 2007, **30**(1), pp. 11-22.
- ³⁸ G.T. Galyon, "Annotated tin whisker bibliography and anthology," *IEEE Transactions on Electronic Packaging Manufacturing*, 2005, **28**(1), pp. 94-122.

- Aisan potentiometer-based pedals (2002-2006 Camry) utilize eutectic tin-lead solders and gold solderability platings. The leads have bright tin platings over copper, and this material combination may produce long whiskers. Exponent measured a maximum whisker length of approximately 400 microns in its sample examinations, and Toyota measured lengths on the order of 2 mm in both tests and in inspections of two shorted units from the field.
- Denso potentiometer-based pedals (e.g. 2008 Toyota Corolla and 2002-2003 Lexus SC430) utilize Au-Ni plating on Cu for pins, Ag-Au plating on Cu for contact brushes, and no Sn plating. These pedals are not susceptible to tin whisker-induced shorting, since they do not use tin.
- Denso Hall Effect sensor based pedals (2007 and later Camry) utilize gold plating, are fully potted in epoxy, and are not susceptible to whisker-induced shorting.
- CTS Hall Effect sensor based pedals (2007 and later Camry) use matte tin plating over nickel and use a 60 micron silicone conformal coating. No conformal coating penetration was noted, and no whiskers longer than 5 microns were measured after chemically removing the conformal coating. A tin whisker able to both penetrate the coating and grow to an adjacent contact would still not short since the adjacent contact is insulated by the conformal coating. Tin whiskers would not have the structural strength to penetrate the coating at its distal end.

Irrespective of tin whisker growth susceptibility, accelerator pedal resistive fault testing was performed to understand the potential shorting mechanism and the power of these mechanisms for explaining reported incidents of unintended acceleration.

4.6.4.2 VPA1 and VPA2 Resistive Faults: Parallel vs. Diverging Slopes

The choice of parallel versus diverging slope designs for pedal sensors has been discussed publicly (e.g. Toyota press conference March 10, 2010).³⁹ Exponent analyzed the engine response of parallel versus diverging slope designs to resistive faults. The following are possible response scenarios to a resistive fault between VPA1 and VPA2:

1. Vehicle at Idle

a. VPA1 increases; VPA2 constant

- i. At idle VPA1 will deviate from its expected value.
- ii. If the rise (deviation) in the voltage of VPA1 exceeds [REDACTED] V, a DTC will be set.
- iii. Increasing VPA1 by [REDACTED] V or less on the 2007 Camry produces barely perceptible acceleration.
- iv. Vehicle response to this fault does not depend on whether the VPA1 and VPA2 signals are parallel or diverging.
- v. The Toyota pedal fault detection system is most sensitive at idle, and permits the lowest allowable deviation in the VPA1 and VPA2 signals, providing identical fault detection regardless of VPA1 and VPA2 profiles (i.e. parallel or diverging).

b. VPA1 constant; VPA2 decreases

- i. VPA2 is used for monitoring the state of the pedal circuit; thus this fault condition will not cause the vehicle to accelerate.
- ii. If a resistive fault occurs, VPA2 will deviate from its expected value.

³⁹ In Toyota vehicles, the throttle position sensors use a diverging slope design while the accelerator pedals use a parallel slope design

c. VPA1 and VPA2 converge

- i. The diagnostic system will detect this fault condition and trigger a DTC.
- ii. The response of the vehicle to this fault condition will be the same irrespective of whether the two pedal output signals are parallel or diverging.

2. Vehicle being driven

a. VPA1 increases; VPA2 constant

- i. If VPA1 increases, the ECM will treat it as a driver request for acceleration. However, as soon as the vehicle starts to accelerate (due to this fault condition), the expected driver response will be to release the pedal.
- ii. At pedal release VPA2 will decrease to its idle value. Although VPA1 will also decrease, it will deviate from its value under normal conditions due to the resistive fault. If this deviation exceeds XXXX V, a DTC will be set. If this deviation is less than XXXX V, it will produce barely perceptible vehicle acceleration (as tested on the L4 2007 Camry).
- iii. The vehicle response to this fault condition is independent of whether the VPA1 and VPA2 signals are parallel or diverging as shown in Figure 39.

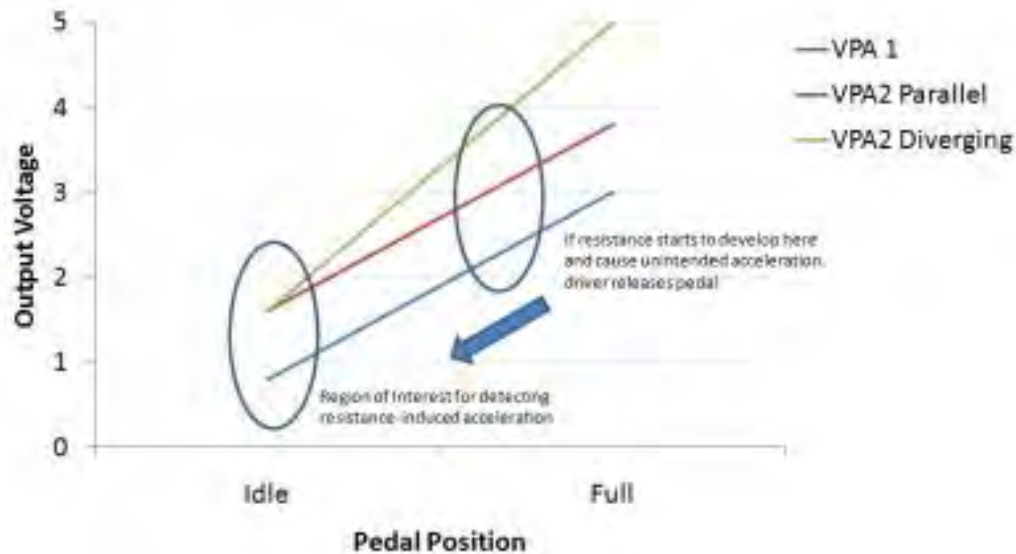


Figure 39. Resistive fault between VPA1 and VPA2 resulting in the VPA1 voltage rising to VPA2. At idle, the deviation is the same for both, parallel or diverging systems.

b. VPA1 constant; VPA2 decreases

- i. A decrease in VPA2 will not cause the vehicle to accelerate.
- ii. If the decrease in VPA2 exceeds a pedal position dependent value, a DTC will be set.
- iii. The response of the vehicle is independent of whether the two pedal output signals are parallel or diverging.

c. VPA1 and VPA2 converge

- i. The diagnostic system will trigger a DTC.
- ii. The response of the vehicle is independent of whether the two pedal output signals are parallel or diverging.

4.6.4.3 Resistive fault testing

Resistive faults on the pedal circuit may result in a deviation in the pedal output signals. A resistive fault may occur between any pair of the six output terminals on the accelerator pedal. Exponent also considered the effects of a resistive fault in series with any of the six pedal output terminals. Figure 40 depicts the six types of resistive faults which have the potential of changing the pedal output signal for VPA1, the signal used by the ECM to determine pedal position. Other resistive faults, such as faults on VPA2's power, ground or signal lines that do not affect VPA1 will not result in vehicle acceleration but may result in setting a DTC.

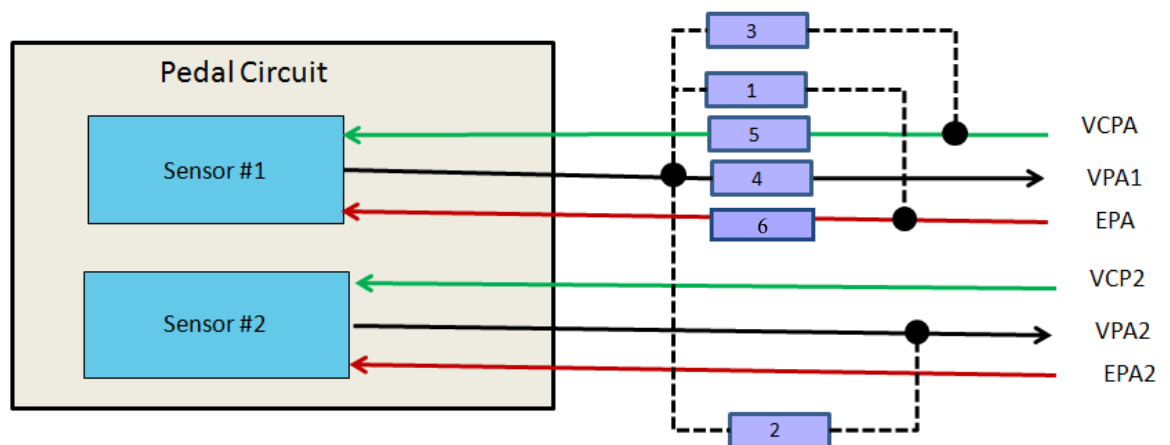


Figure 40. Single point resistive fault conditions that can affect VPA1 ⁴⁰ (the purple boxes indicate the location of the resistive fault for each fault condition).

The six resistive faults depicted in Figure 40 are:

1. Output to Ground: VPA1 (or VPA2) to EPA (or EPA2)
2. Output to Output: VPA1 to VPA2
3. Output to +5 V: VPA1 (or VPA2) to VCPA (or VCP2)
4. Series resistance on VPA1 (or VPA2)

⁴⁰ Many of the depicted fault conditions are physically improbable requiring multiple protection layers to be compromised. Such scenarios are included for completeness. A resistive fault between VPA1 and EPA2 (ground) would have the same effect as a resistive fault between VPA1 and EPA1.

5. Series resistance on +5 Vdc (VCPA or VCP2)
6. Series resistance on Ground (EPA or EPA2)

4.6.4.4 Resistive Fault between Output and Power Supply Terminals (Faults 1 and 3)

Potentiometer Pedal—Figure 41 shows the response of a potentiometer pedal to an induced variable resistive fault between VPA1 (or VPA2) and the supply terminals.

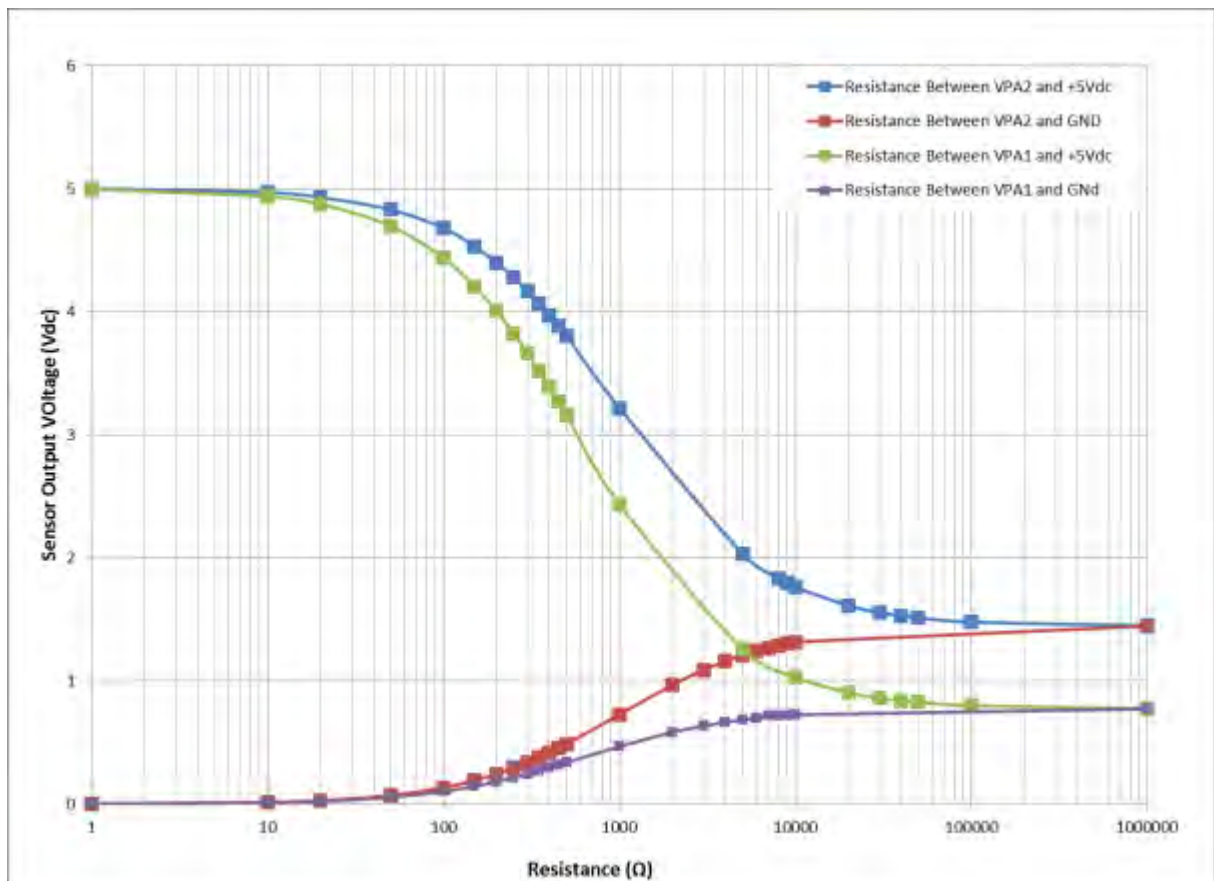


Figure 41. Potentiometer pedal output voltage with fault resistance to +5 Vdc terminal or ground terminal (GND).

Testing (2002 V6 Camry) also demonstrated:

- A resistive fault between VPA2 and VCP2 produced a rise in VPA2. As expected, a rise in the VPA2 signal did not increase engine rpm. A DTC (P1121) was triggered for a resistive fault of less than 10 k Ω between VPA2 and VCP2. No change in engine rpm was observed for resistance values higher than 10 k Ω .
- A resistive fault between VPA1 and VCPA produced a rise in VPA1. A DTC (P1121) was triggered for a resistive fault of less than 10 k Ω between VPA1 and VCPA. The rise in the VPA1 signal for a resistive fault of more than 10 k Ω did not lead to a measurable rise in the engine rpm (the rise in the VPA1 signal was less than 0.2 V).⁴¹
- For a resistive fault between VPA1 and ground (EPA), a drop in VPA1 occurred, causing VPA1 to be lower than its normal value, resulting in vehicle slowing (while being driven) as the ECM interprets this as a smaller pedal depression demand. A DTC (P1121) was triggered for resistance values less than 6 k Ω between VPA1 and EPA.
- A DTC (P1121) was triggered for a resistive fault of less than 10 k Ω between VPA2 and ground (EPA2). No measurable engine rpm change was observed for resistance values that were greater than 10 k Ω .

⁴¹ The vehicle continued to remain at idle since the value of the VPA2 signal did not rise, which the ECM interpreted as an idle speed condition.

CTS Pedal—Figure 42 shows the CTS pedal response to a resistive fault between VPA1 (or VPA2) and the supply terminals.

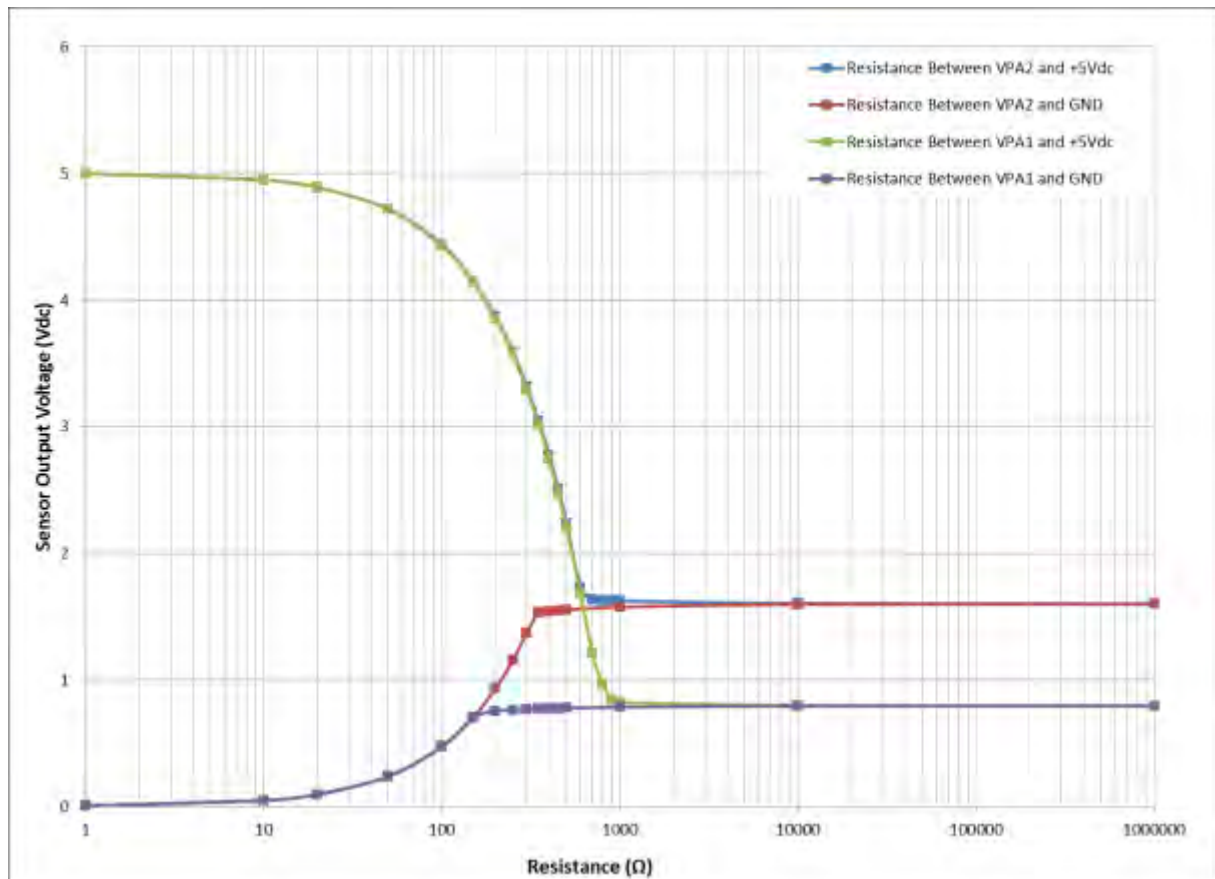


Figure 42. CTS pedal output voltage as a function of fault resistance to +5 Vdc or ground.

Testing (2007 V6 Camry) demonstrated:

- A resistive fault between VPA2 and VCP2 resulted in a rise in VPA2. As predicted, raising VPA2 did not increase engine rpm. A DTC (P2121) was triggered for a resistive fault of less than approximately 500 Ω between VPA2 and VCP2. No change in engine rpm was observed for resistance values higher than approximately 500 Ω.
- A resistive fault between VPA1 and VCPA1 resulted in a rise in VPA1. A DTC (P2121) was triggered for a resistive fault of less than approximately

800 Ω . The rise in the VPA1 signal for a resistive fault of more than 800 Ω did not lead to a rise in engine rpm.⁴²

- A resistive fault between VPA1 and ground (EPA), resulted in a drop in VPA1 below its normal value, resulting in the vehicle slowing down (while being driven) as the ECM interprets this as a smaller pedal depression. A DTC (P2121) was triggered for resistance values less than approximately 500 Ω .
- A DTC (P2121) was triggered for a resistive fault of less than approximately 500 Ω between VPA2 and ground (EPA2). No engine rpm change was observed for resistance values greater than approximately 500 Ω .

⁴² The vehicle continued to remain at idle since the VPA2 did not rise due to the resistive fault.

Denso Pedal—Figure 43 shows the Denso pedal response to a resistive fault between VPA1 (or VPA2) and the supply terminals.

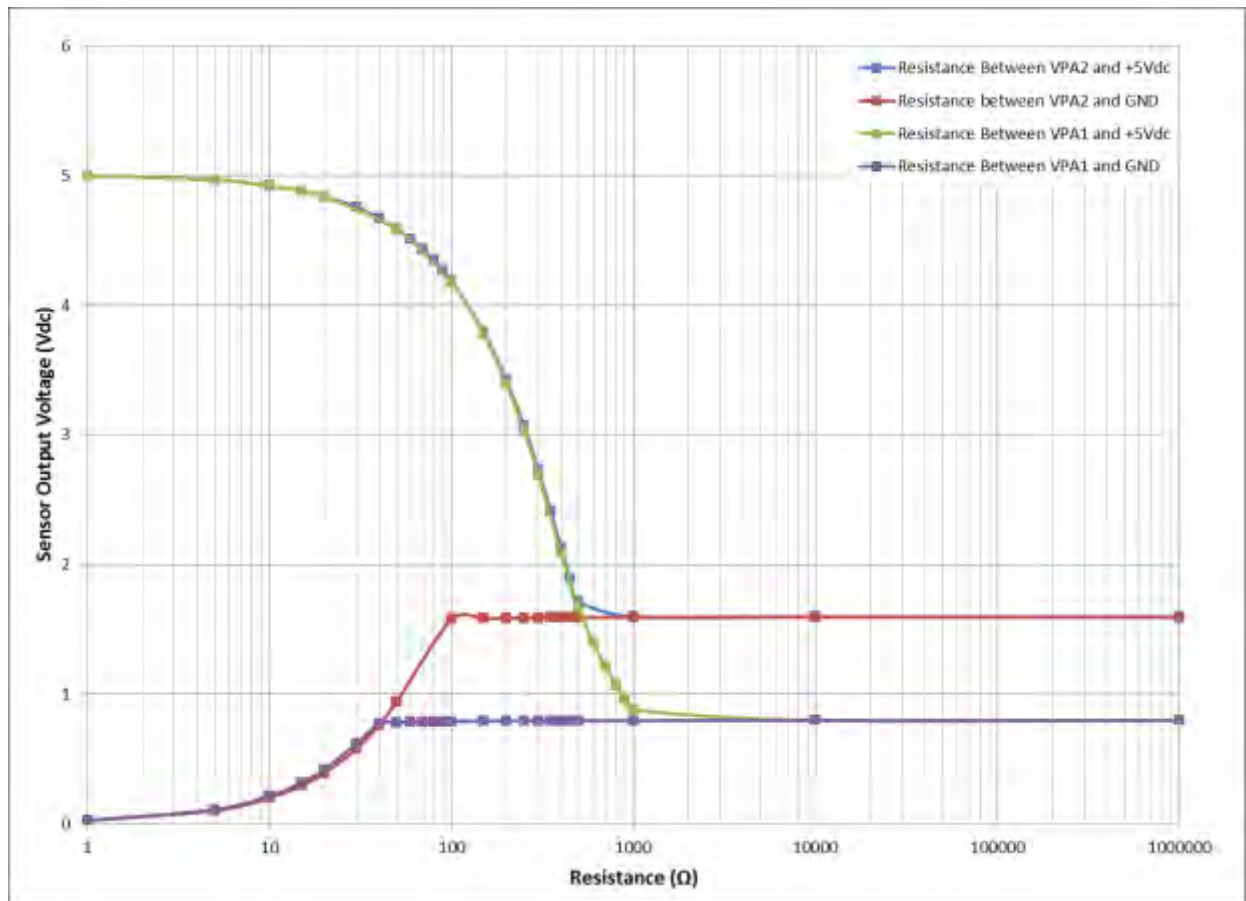


Figure 43. Denso pedal output voltage as a function of fault resistance to +5 Vdc or ground.

Testing (2007 L4 Camry) demonstrates:

- A resistive fault between VPA2 and VCP2 resulted in a rise in VPA2 but as predicted did not lead to an increase in engine rpm. A DTC (P2121) was triggered for a resistive fault of less than 500 Ω between VPA2 and VCP2. No change in engine rpm was observed for resistance values greater than approximately 500 Ω .
- A resistive fault between VPA1 and VCPA1 resulted in a rise in VPA1. A DTC (P2121) was triggered for a resistive fault of less than approximately 800 Ω . No change in engine rpm was observed for resistance values greater than approximately 800 Ω .⁴³
- A resistive fault between VPA1 and ground (EPA), pulls down VPA1, making it lower than its value under normal operating conditions and causing the vehicle to slow down as the ECM interprets this as a smaller pedal depression. A DTC (P2121) was triggered for resistance values less than approximately 90 Ω .
- A DTC (P2121) was triggered for a resistive fault of less than approximately 300 Ω between VPA2 and ground (EPA2). No engine rpm change was observed for resistance values greater than 300 Ω .

4.6.4.5 Resistive Faults between VPA1 and VPA2 (Fault 2)

Electrical testing of each pedal type was conducted to determine the pedal response for resistive faults between VPA1 and VPA2. The response of each pedal type will be discussed individually.

⁴³ This was because the vehicle continued to remain at idle since VPA2 did not rise.

Potentiometer Pedals—The pedal response to a resistive fault between VPA1 and VPA2 was characterized for three pedal positions:

1. No depression (idle)
2. Pedal depressed with VPA1 at approximately 1.5 V
3. Pedal depressed with VPA1 at approximately 3.0 V.

Figure 44 illustrates the pedal response.

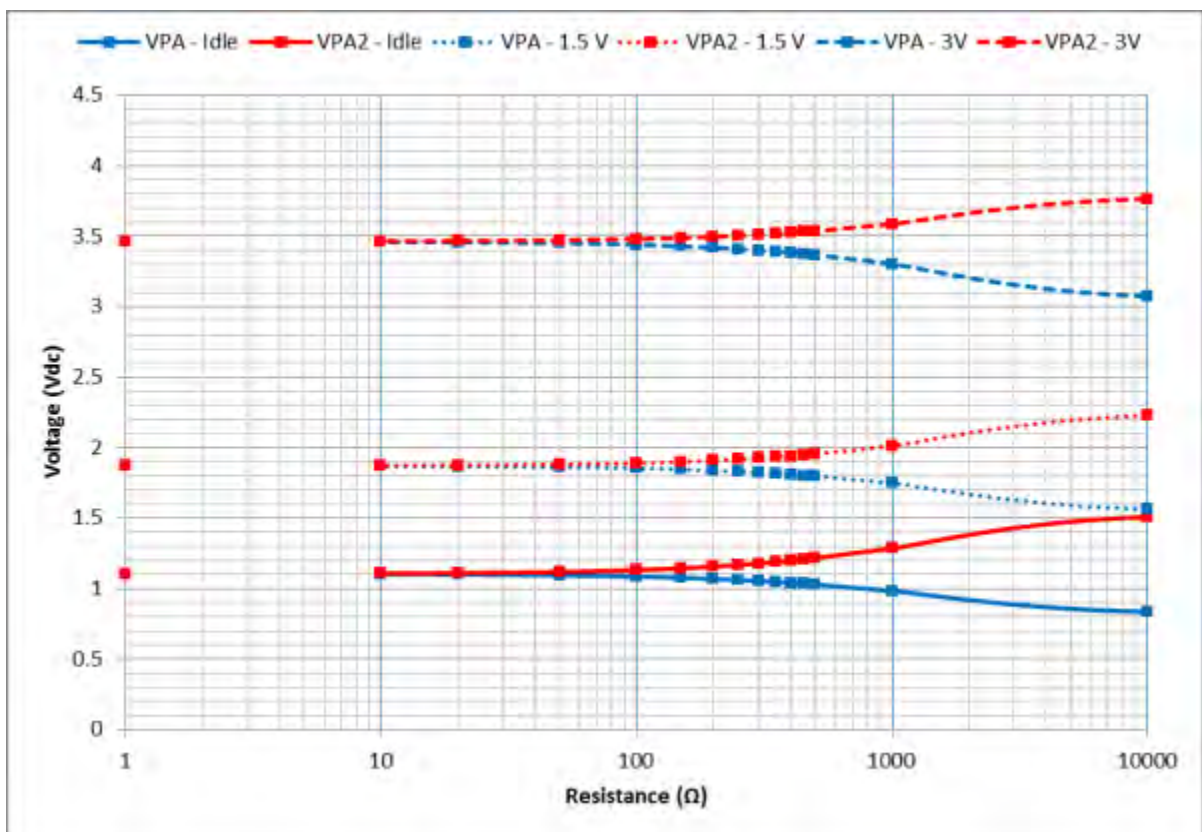


Figure 44. Resistive fault between VPA1 and VPA2 for a potentiometer pedal.

Testing (on a 2002 V6 Camry with the vehicle at idle) demonstrated that:

- A DTC (P2121) was triggered for resistance values less than approximately 2 kΩ

- For fault resistances decreasing from very high values down to 2 k Ω , VPA1 increased by approximately 0.1 V and was brought closer to VPA2, producing a slight engine RPM increase (Figure 44).
- For all resistances, releasing the pedal returned VPA1 to a voltage of a low value consistent with the engine in an idle or high idle condition.⁴⁴ Thus, this failure mode will not lead to UA.

CTS Pedal—The pedal response to a resistive fault between VPA1 and VPA2 was characterized for three pedal positions

1. No depression (idle)
2. Pedal depressed such that VPA1 at approximately 1.5 V
3. Pedal depressed such that VPA1 at approximately 3.0 V.

Figure 45 illustrates the pedal response.

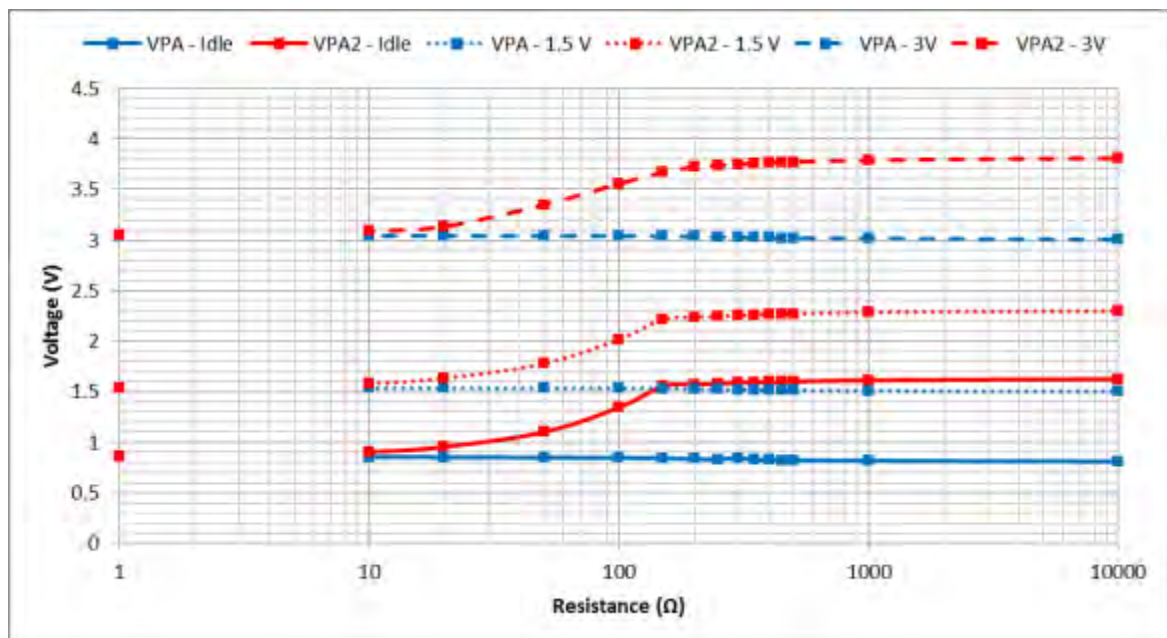


Figure 45. Resistive fault between VPA1 and VPA2 for a CTS pedal.

⁴⁴ Less than approximately 1200 rpm for a V6 2002 Camry tested

Testing (on a 2007 V6 Camry with the vehicle at idle) demonstrated that:

- No change in VPA1 occurred when a resistance was introduced between VPA1 and VPA2. The lack of change in VPA1 translated into normal operation for the vehicle. A DTC (P2121) was triggered for resistance values less than approximately 100 Ω .

Denso Pedal—The pedal response to a resistive fault between VPA1 and VPA2 was characterized for three pedal positions

1. No depression (idle)
2. Pedal depressed such that VPA1 at approximately 1.5 V
3. Pedal depressed such that VPA1 at approximately 3.0 V.

Figure 46 illustrates the pedal response.

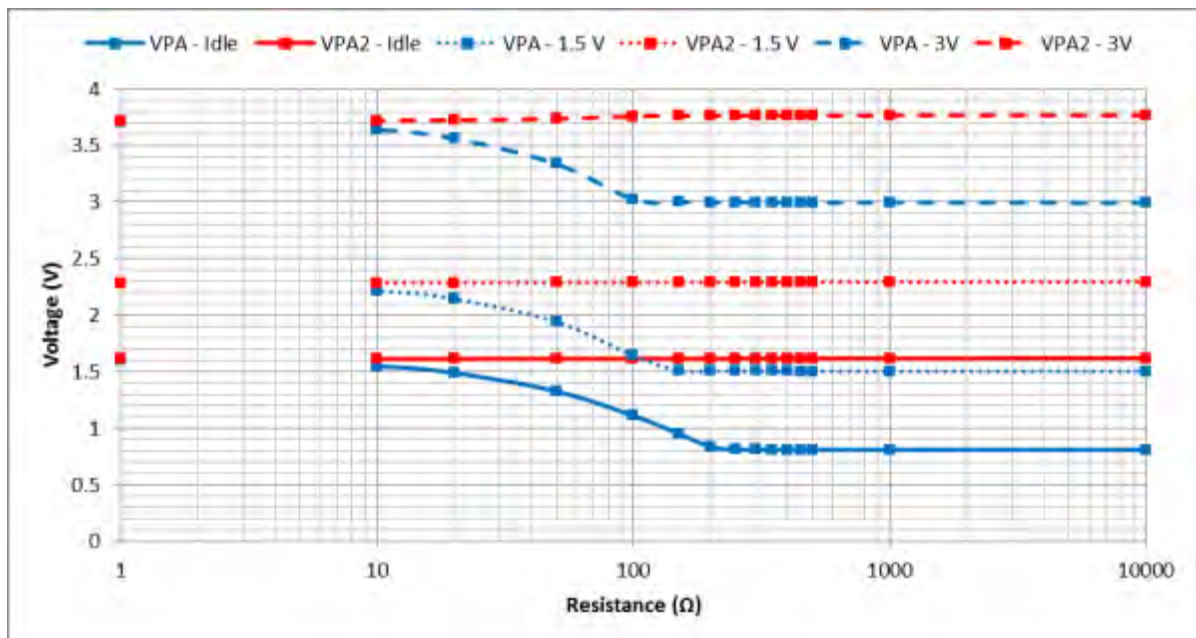


Figure 46. Resistive fault between VPA1 and VPA2 for a Denso pedal.

Testing (on a 2007 L4 Camry with the vehicle at idle) demonstrated that:

- Minimal change in VPA2 was observed due to the resistive fault, with VPA1 converging toward VPA2 as the fault resistance was reduced.
- No change in vehicle behavior was observed for resistance values greater than approximately 250 Ω . Even though VPA1 rises, the engine rpm does not increase because the ECM monitors both signals and only transitions the vehicle from idle when idle flags for both VPA1 and VPA2 clear. Since VPA2 stays at idle value, the vehicle continues in idle mode.
- A DTC (P2121) was triggered for all resistance values less than 100 Ω
- Between 100 Ω and 250 Ω , VPA1 increases towards VPA2. If the fault is present before the ignition is turned on, the pedal position learning algorithm (discussed in section 4.5) may learn the new VPA1 and VPA2 and RPM would not change. If learning does not occur at ignition on, the history of the learned values will be used as the new learned values. Regardless of whether learning occurs at ignition on, VPA2 stays at the idle value and engine rpm will not increase with the pedal released.
- For all fault resistances, releasing the pedal returned VPA1 to a voltage of a low value consistent with the engine in an idle or high idle condition⁴⁵; UA would not result from this failure mode.

4.6.4.6 Series Resistance on VPA1 (Fault 4)

VPA1 provides pedal position to the ECM which filters it. In addition, a pull-down resistor on the ECM causes VPA1 to be pulled to ground in the event of an open-circuit fault on the pedal circuit. A series fault resistance on the VPA1 circuit will lead to a drop in the VPA1 signal,

⁴⁵ Less than approximately 1200 rpm on the 2007 L4 Camry tested

causing the vehicle to slow down as the driver request received by the ECM will be lower.⁴⁶ If this drop exceeds approximately 0.4 V, a DTC will be triggered and the vehicle will transition to the limp-home mode (see section 4.4).

4.6.4.7 Series resistance on VCPA (Fault 5)

VCPA provides power to the pedal sensors. A resistance in series with VCPA (and/or VCP2) causes a drop in the power supply voltage to the potentiometer/Hall Effect sensors, causing the system to:

- Decrease the supply voltage to the circuit generating VPA1 if a series resistance fault occurs on VCPA. This reduces VPA1 for the same pedal position for both potentiometer and Hall Effect (both CTS and Denso) pedal outputs. A drop in the magnitude of VPA1 will be interpreted by the ECM as a reduction in driver demand. The magnitude of the drop will depend on the fault resistance magnitude. If the drop in VPA1 exceeds a threshold⁴⁷ (while the vehicle is at idle), a DTC will be triggered and the vehicle will transition to the limp-home mode.
- Decrease the supply voltage to the circuit generating VPA2 if a series resistance fault occurs on VCP2. This reduces VPA2 for the same pedal position for both potentiometer and Hall Effect (both CTS and Denso) pedal outputs. VPA2 is used by the ECM to monitor the circuit generating VPA1. Hence, a drop in VPA2 will not affect the throttle opening position. If the drop in VPA2 exceeds a threshold⁴⁸ (while the vehicle is at idle), a DTC will be triggered and the vehicle will transition to the limp-home mode.

⁴⁶ If the series fault resistance occurs before the ignition is turned on and causes a small drop in the VPA1 signal, this will be learnt by the ECM as the idle position value at ignition turn on and the vehicle will continue to operate as normal. See section 4.4 for more details.

⁴⁷ Refer to section 4.4 for pedal related DTC triggers and threshold values.

⁴⁸ Refer to section 4.4 for pedal related DTC triggers and threshold values.

4.6.4.8 Series resistance on EPA (EPA2) (Fault 6)

The EPA terminal provides the ground for the pedal position sensor circuits. A resistance in series with the EPA (and/or EPA2) input causes a change in the power supply voltage drop across the potentiometer/Hall Effect sensors. The system response to this condition would be as follows:

Potentiometer Pedal—A series resistance fault on the EPA circuit changes the voltage across the circuit that generates VPA1 and causes a rise in VPA1 as shown in Figure 47. The magnitude of the rise in VPA1 is a function of the magnitude of the resistance. DTC P1121 was triggered for resistance values higher than approximately 200 Ω on a 2002 V6 Camry. The rise in the value of VPA1 for resistance values smaller than 200 Ω did not result in an increase in engine rpm, as this fault condition caused no change in the value of VPA2, causing the vehicle to continue to remain at idle.

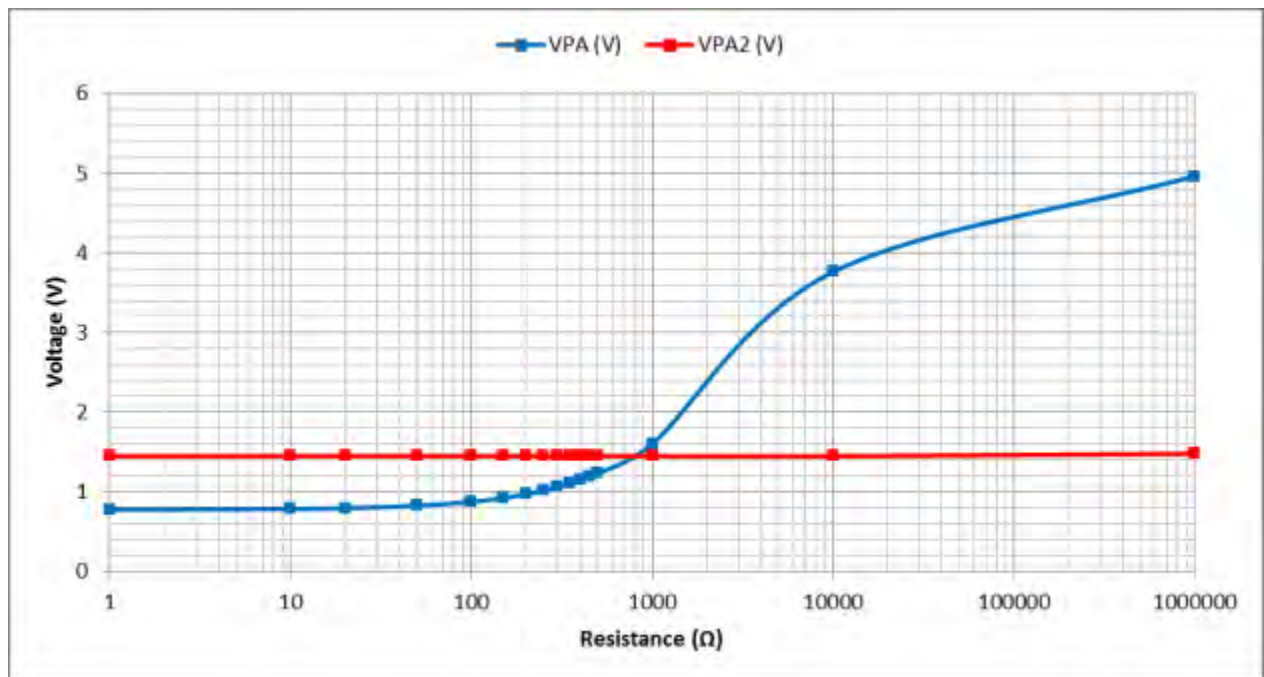


Figure 47. Resistive fault in series with EPA for a potentiometer pedal.

A series resistance fault on the EPA2 circuit changes the voltage across the circuit that generates VPA2 and causes a rise in VPA2 as shown in Figure 48. The magnitude of rise in VPA2 is a function of the magnitude of the resistance. Since the ECM uses VPA1 for throttle control, this rise in VPA2 does not affect engine rpm. DTC (P1121) was triggered for resistance values higher than approximately 250 Ω on a 2002 V6 Camry. No change in engine rpm was observed for resistance values that were lower than 250 Ω .

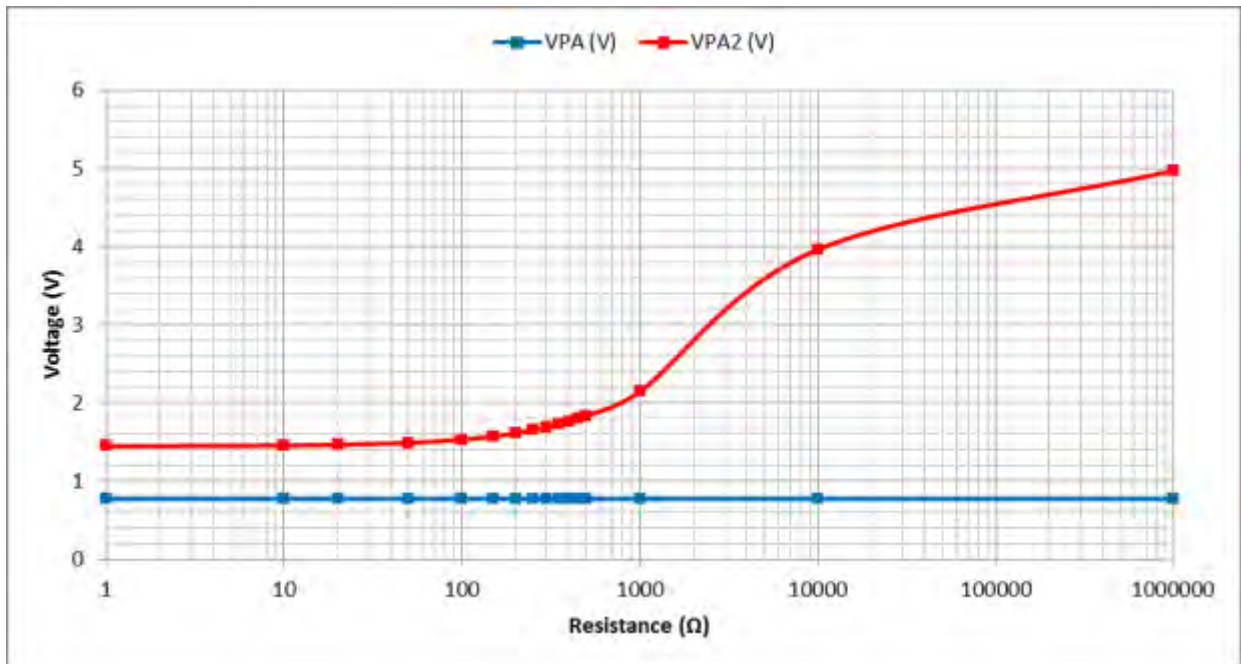


Figure 48. Resistive fault in series with EPA2 for a potentiometer pedal.

CTS Pedal—A series resistance fault on the EPA circuit changes the voltage across the circuit that generates VPA1 and causes a rise in VPA1 as shown in Figure 49. The magnitude of the rise in VPA1 is a function of the magnitude of the resistance. DTC P2121 was triggered for resistance values higher than approximately 40 Ω on a 2007 V6 Camry. The rise in the value of VPA1 for resistance values that were smaller than 40 Ω did not result in an increase in engine rpm as this fault condition caused no change in the value of VPA2 causing the vehicle to continue to remain at idle.

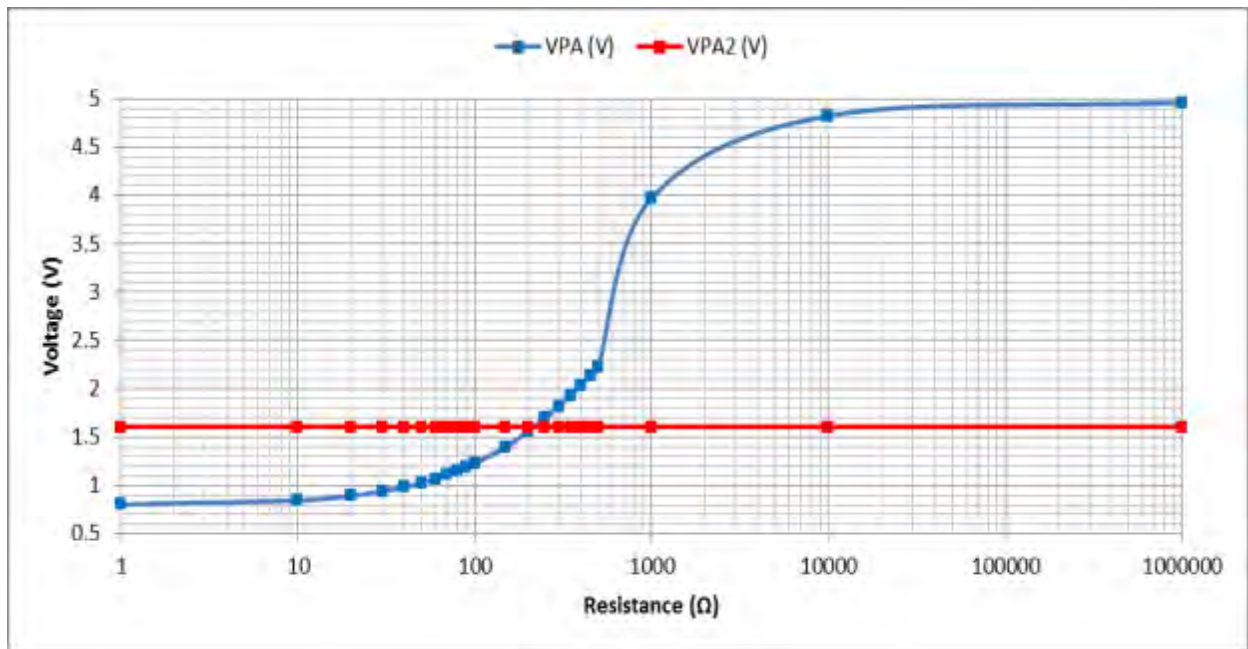


Figure 49. Resistive fault in series with EPA for a CTS pedal.

A series resistance fault on the EPA2 circuit changes the voltage across the circuit that generates VPA2 and causes a rise in VPA2 as shown in Figure 50. The magnitude of rise in VPA2 is a function of the magnitude of the resistance. Since the ECM uses VPA1 for throttle control, this rise in VPA2 does not affect engine rpm. DTC P2121 was triggered for resistance values higher than approximately 50 Ω on a 2007 V6 Camry. No change in engine rpm was observed for resistance values lower than 50 Ω .

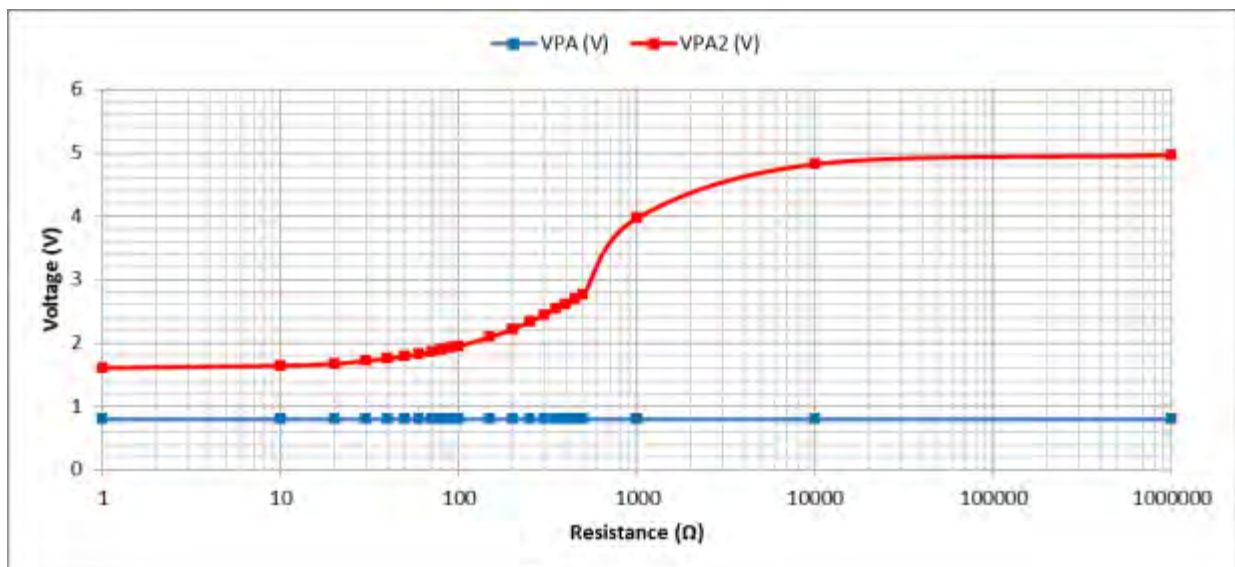


Figure 50. Resistive fault in series with EPA2 for a CTS pedal.

Denso Pedal—A series resistance fault on the EPA circuit changes the voltage across the circuit that generates VPA1 and causes a rise in VPA1 as shown in Figure 49. The magnitude of the rise in VPA1 is a function of the magnitude of the resistance. DTC P2121 was triggered for resistance values higher than approximately 30 Ω on a 2007 L4 Camry. The rise in the value of VPA1 for resistance values smaller than 30 Ω did not result in an increase in engine rpm as this fault condition caused no change in the value of VPA2; the vehicle remained at idle.

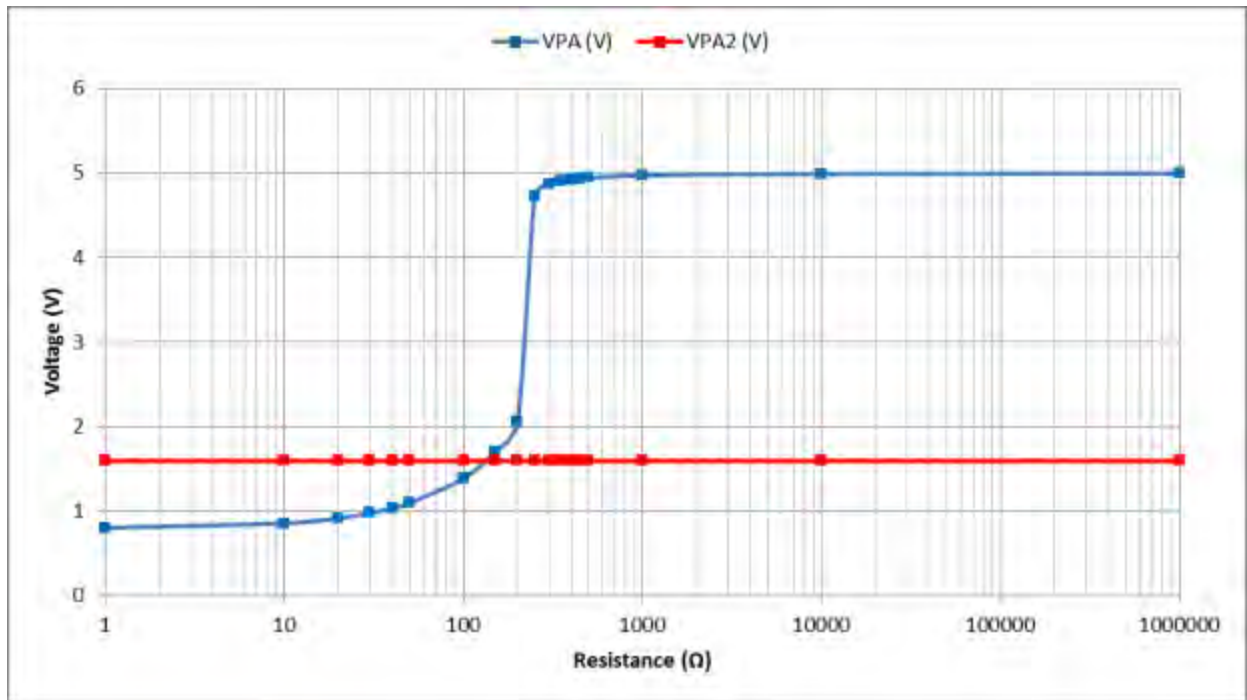


Figure 51. Resistive fault in series with EPA for a Denso pedal.

A series resistance fault on the EPA2 circuit changes the voltage across the circuit that generates VPA2 and causes a rise in VPA2 as shown in Figure 52. The magnitude of rise in VPA2 is a function of the magnitude of the resistance. Since the ECM uses VPA1 for throttle control, this rise in VPA2 does not affect engine rpm. DTC P2121 was triggered for resistance values higher than approximately 40 Ω on a 2007 L4 Camry. No change in engine rpm was observed for resistance values that were lower than 40 Ω .

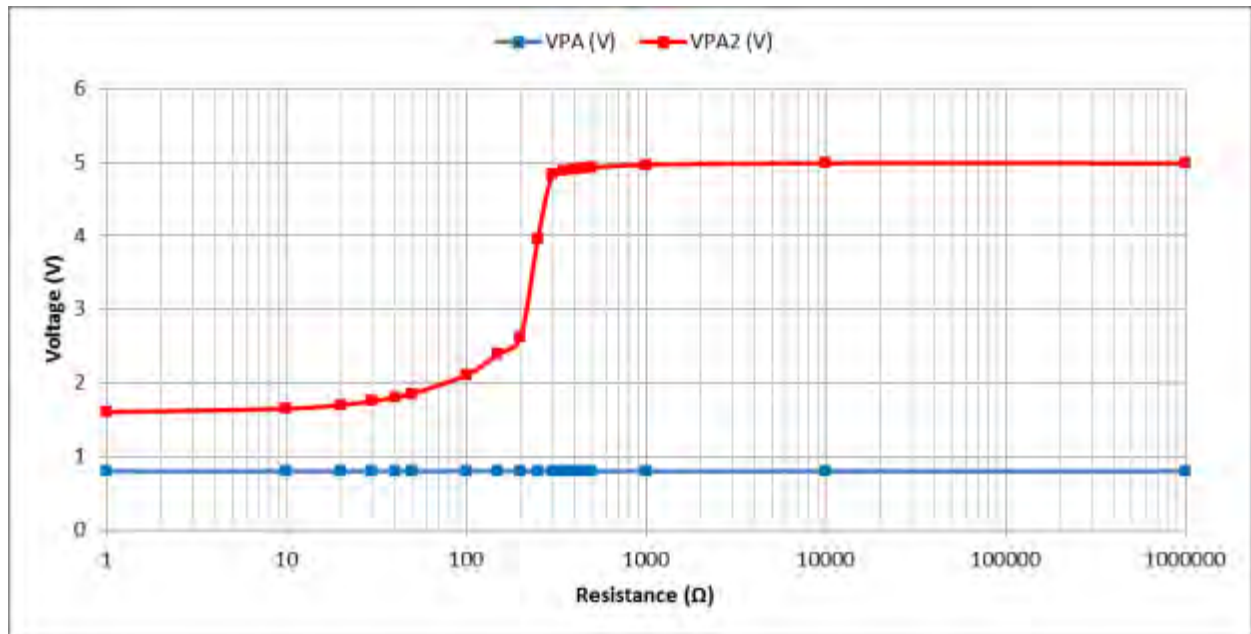


Figure 52. Resistive fault in series with EPA2 for a Denso pedal.

A single resistive fault in the accelerator pedal circuit, regardless of the mechanism, can neither replicate nor explain reported incidents of unintended acceleration. Simultaneous resistive faults in both the VCPA and VCP2 signals are discussed in detail in Section 4.7.

4.6.5 Power Supply Variations

Both potentiometers and Hall Effect sensors on pedal circuits require 5 V power from the ECM for operation. The ECM 5 V power supply used by the pedal circuits also powers various other components (including the processors, the throttle motor driver IC and various sensors). Power supply malfunctions can potentially lead to one of the following conditions:

1. Power supply under-voltage
2. Power supply over-voltage
3. Noisy power supply.

4.6.5.1 Power Supply Under-Voltage

The pedal circuit under-voltage response is a function of pedal type.

Potentiometer Pedals—VPA1 and VPA2 ratiometrically track the +5.0 Vdc power supply voltage, as it decreases to zero volts (Figure 53)

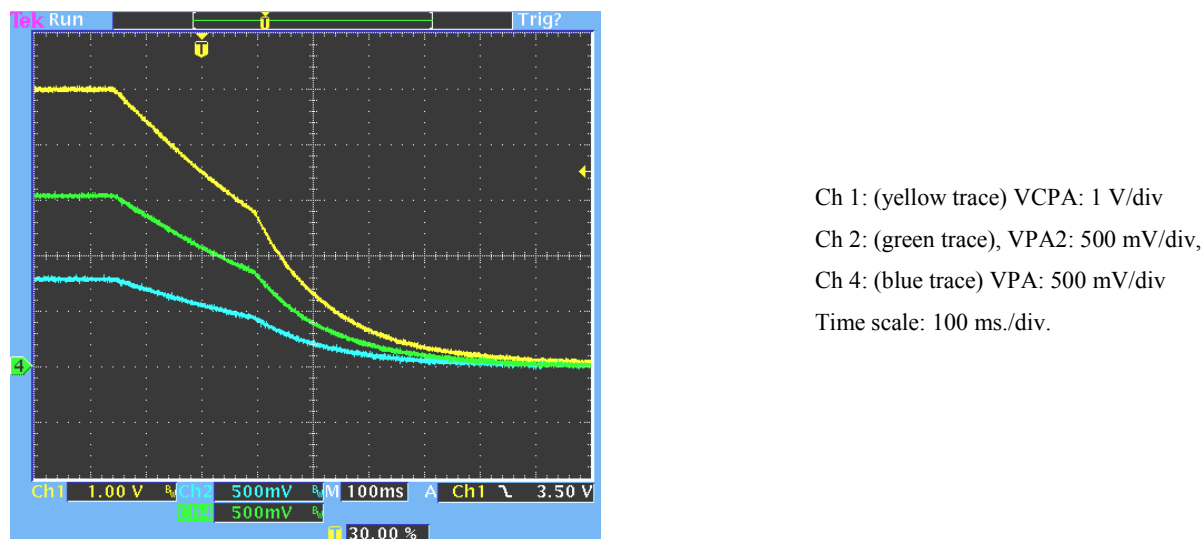


Figure 53. Low voltage operation of the potentiometer pedal.

A power supply under-voltage condition pulls down VPA1 and VPA2, causing the vehicle to slow down as the ECM receives signals corresponding to a smaller pedal depression. In addition, a drop in the power supply voltage reduces the difference between VPA1 and VPA2. A DTC is triggered if this difference is less than a threshold⁴⁹, and the vehicle transitions to the Class 1.5 limp-home mode.

⁴⁹ Refer to the pedal related fail-safes section (section 4.4) for a complete discussion on the DTC that will be triggered and threshold values that will trigger this DTC.

CTS Pedals—The response of the CTS pedal to an under-voltage condition is as follows:

- VPA1 and VPA2 ratiometrically track the +5.0 Vdc power supply voltage down to approximately 2.8 Vdc⁵⁰ (Figure 54)
- Below approximately 2.8 Vdc, VPA1 and VPA2 are almost identical.

Figure 54 shows VPA1 and VPA2 output voltages as the +5.0 Vdc power supply is gradually decreased to zero volts.

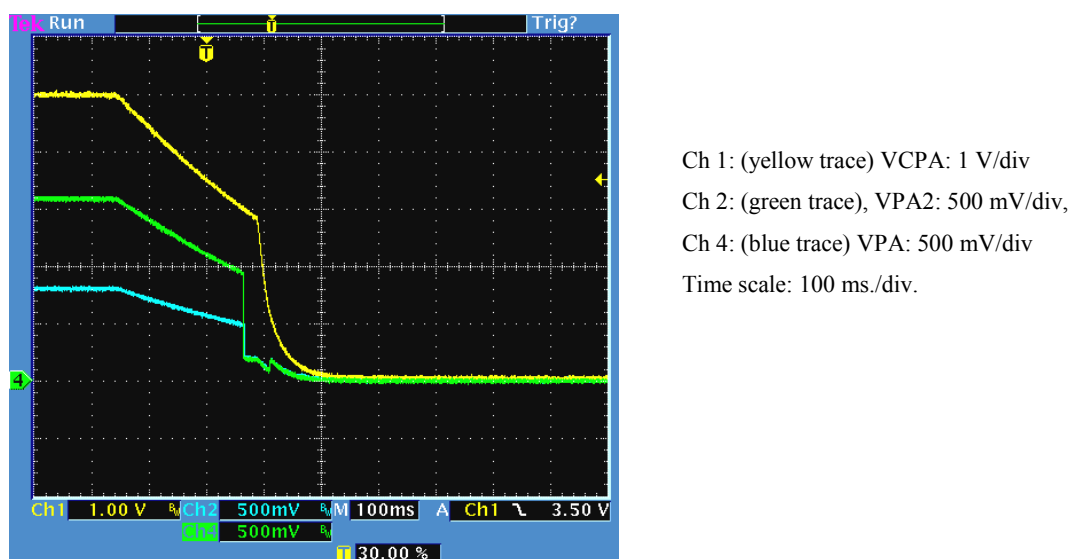


Figure 54. Output voltage v. supply voltage for CTS Pedal.

A power supply under-voltage condition pulls down VPA1 and VPA2, causing the vehicle to slow down as the ECM receives signals corresponding to a smaller pedal depression. If the voltage drops below approximately 2.8 Vdc, VPA1 and VPA2 become identical, triggering a DTC and transitioning the vehicle to the Class 1.5 limp-home mode.

Hence, for a CTS pedal, an under-voltage condition would cause the pedal output signals to be lower than their values under normal operating conditions. This would cause the vehicle to

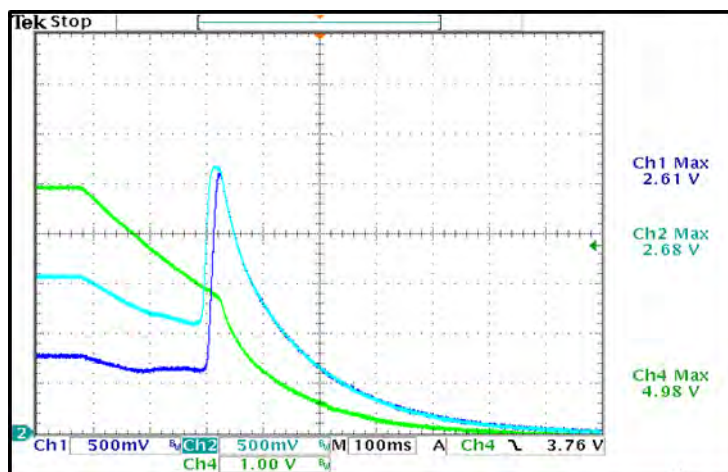
⁵⁰ Under overload conditions, if the +5 Vdc supply, is reduced to XXXX Vdc or below, the power supply IC generates a reset pulse that will reset the Main and Sub processors. This condition activates different levels of fail safes, resulting in the engine shutting off. This will be discussed in detail in section 6.6 of the report.

slow down as the ECM would receive a signal corresponding to a smaller pedal depression. If the voltage drops below ~ 2.8 Vdc, VPA1 and VPA2 would be identical. This would set a DTC and transition the vehicle to a Class 1.5 limp-home mode.⁵¹

Denso Pedals—The response of the Denso pedal to an under-voltage condition is as follows:

- VPA1 and VPA2 ratiometrically track the +5.0 Vdc power supply voltage down to approximately 3.0 Vdc
- At approximately 2.9 Vdc, VPA1 and VPA2 increase to the power supply voltage
- When the power supply decreases below approximately 2.8 Vdc, VPA1 and VPA2 are almost identical and decrease simultaneously.

Figure 55 shows VPA1 and VPA2 voltages of the Denso pedal as the +5.0 Vdc power supply voltage is gradually decreased to zero volts.



Ch 1: (dark blue trace) VPA: 500mV/div
 Ch 2: (light blue trace), VPA2: 500 mV/div,
 Ch 4: (green trace) VCPA: 1.00 V/div
 Time scale: 100 ms./div.

Figure 55. Output voltage v. supply voltage for Denso Pedal.

⁵¹ Discussed in detail in a subsequent section.

A power supply under-voltage condition pulls down VPA1 and VPA2, causing the vehicle to slow down as the ECM receives signals corresponding to a smaller pedal depression. If the voltage drops below ~ 2.9 V, VPA1 or VPA2 may rise to the power supply rail. If the voltage drops below ~ 2.8 Vdc, VPA1 and VPA2 become identical, resulting in the triggering of a DTC and the transitioning of the vehicle to a Class 1.5 limp-home mode⁵².

In the remote possibility of the power supply voltage decreasing toward the narrow window between 2.9 V and 2.8 V where VPA1 might rise to the power supply voltage before VPA2, other limp-homes would be activated which would result in the vehicle transitioning to the limp-home mode.

As the +5 Vdc power supply decreases to approximately 3.5 Vdc, the power supply IC generates a reset pulse which resets the Main and Sub processors. Resetting the processors activates fail safes, shutting the engine off and preventing UA (section 6.6.3.3).

4.6.5.2 Power Supply Over-Voltage

The +5 Vdc power supply IC maximum output rating is 5.065 V. An additional 0.065V in output will not impact the vehicle. Power supply IC failure modes may result in an output voltage that exceeds the maximum rating and result in readily detected permanent IC damage, a situation inconsistent with reported incidents of unintended acceleration. In the hypothetical event that the power supply fails such that its output exceeds rated specifications without causing a permanent failure of the IC, the over-voltage condition may cause components on the ECM to behave abnormally as discussed in detail in section 6.6.3.4.

4.6.5.3 Effect of Noise on Power Supply Outputs

Design features in both the pedal circuitry and in the ECM provide protection against excessive noise and/or ripple on the power supply (section 6.6.3). Testing performed to characterize vehicle response to power supply noise is detailed in a separate Exponent report. The testing

⁵² This will be discussed in detail in a subsequent section.

performed did not identify any root cause that would explain reported incidents of unintended acceleration.

4.7 Multiple Failures⁵³

Exponent prepared a report analyzing a specific case of multiple faults alleged to be a possible cause for reported incidents of unintended acceleration.⁵⁴ To induce UA, the pedal circuitry had to be artificially faulted in a complex and specific fault sequence, using specific resistance values. Most of the hypothesized “faults” result in a detected problem (e.g. triggering a DTC and a limp-home mode of operation) and/or leave unmistakable physical evidence that would not disappear when the ignition key was cycled. Exponent’s inspections of used vehicle parts, vehicles alleged to have experienced unintended acceleration, warranty database, and testing (of vehicles and individual components) have found no evidence that such multiple failures occur in the field.

The relationships between the identified fault events are captured in the fault tree diagram in Figure 56, and in the event flowchart shown in Figure 57. No evidence was found that supported this scenario as the root cause of reported unintended acceleration events⁵⁵.

Exponent, Toyota, and NHTSA have continued searching for evidence of this scenario, including performing electrical measurements on vehicles that drivers reported an unintended acceleration, review and inspection of components, and review of warranty data. To date, no evidence has been found that even a single reported event occurred due to this scenario.

⁵³ Portions of this section are summarized from Exponent’s report, titled, “Evaluation of Gilbert Demonstration”, dated March 2010.

⁵⁴ “Evaluation of Gilbert Demonstration”, March 2010.

⁵⁵ “Evaluation of Gilbert Demonstration”, March 2010.

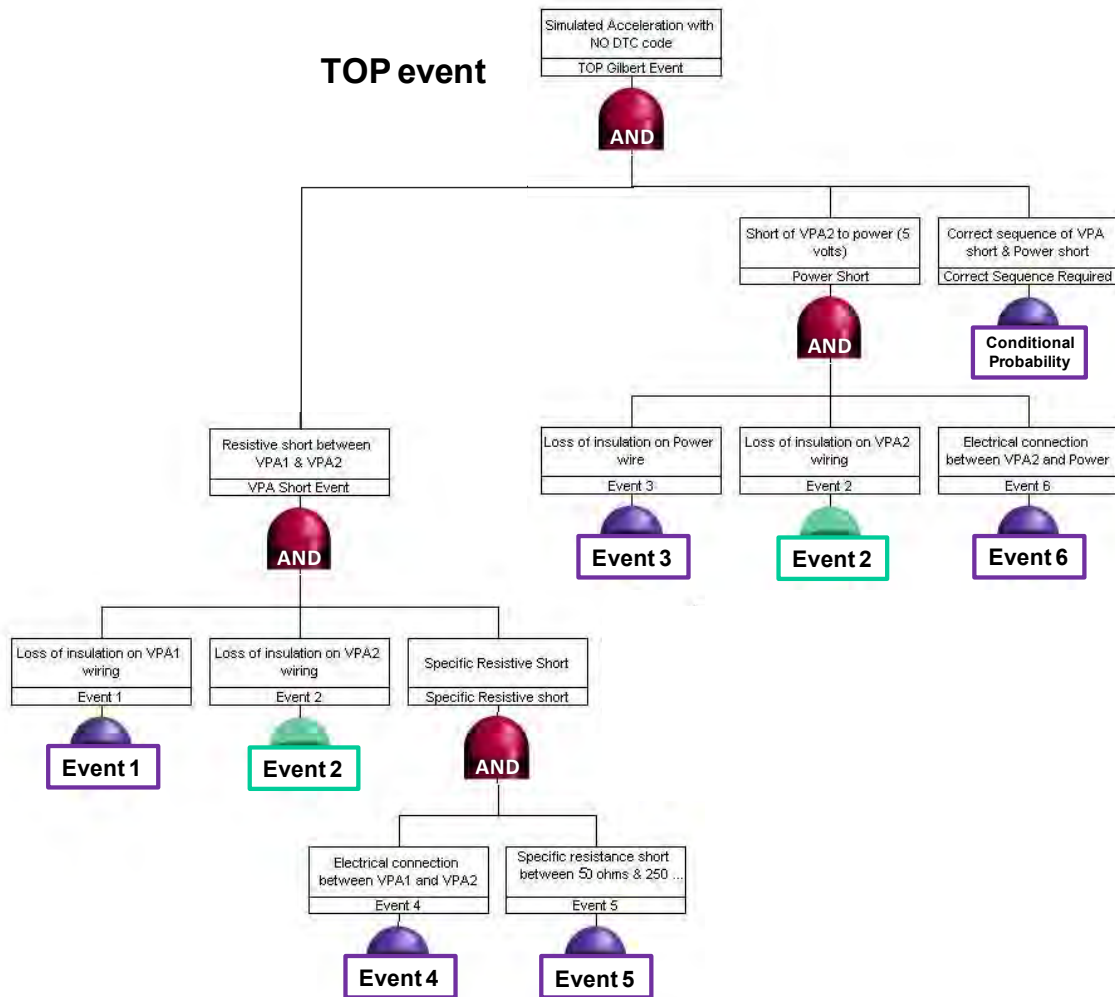


Figure 56. Fault tree analysis of simultaneous pedal circuit resistive faults (Avalon).

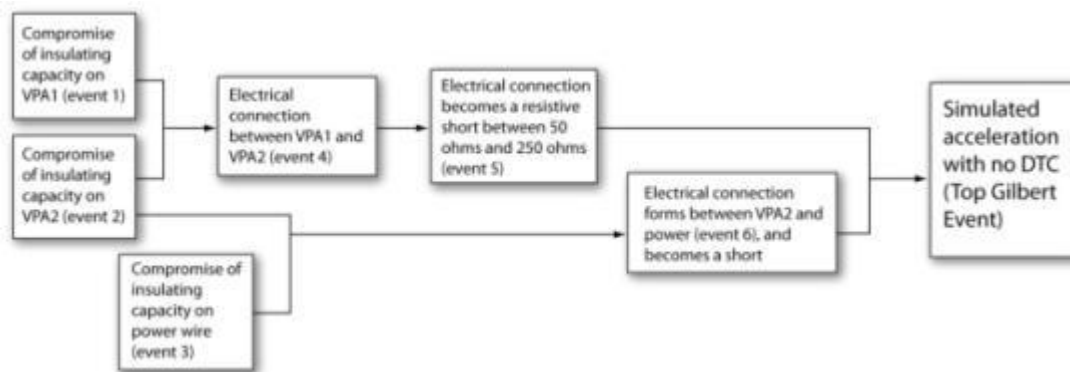


Figure 57. Flowchart of events for simultaneous pedal circuit resistive faults (Avalon).

4.8 Resistive Faults between VPA1 and VPA2 and Vehicle Behavior on Restart

Depending on the accelerator pedal sensor, a resistive fault between VPA1 and VPA2 will reduce their 0.8 V nominal difference (section 5.6.4) leading to:

- In Potentiometer pedals
 - A rise in VPA1 and a corresponding drop in VPA2 eventually triggering DTC P2121 (P1121 for 2002 model year vehicles).
- In Denso pedals
 - No change in VPA2 signal and a rise in VPA1 eventually triggering DTC P2121.
- In CTS Pedals
 - No change in VPA1 and a drop in VPA2 eventually triggering DTC P2121.

The vehicle enters the limp-home mode when DTC P2121 (or P1121) is triggered; in this mode, depressing the brake pedal causes the throttle request from the pedal to return to 0°, regardless of the accelerator pedal request.

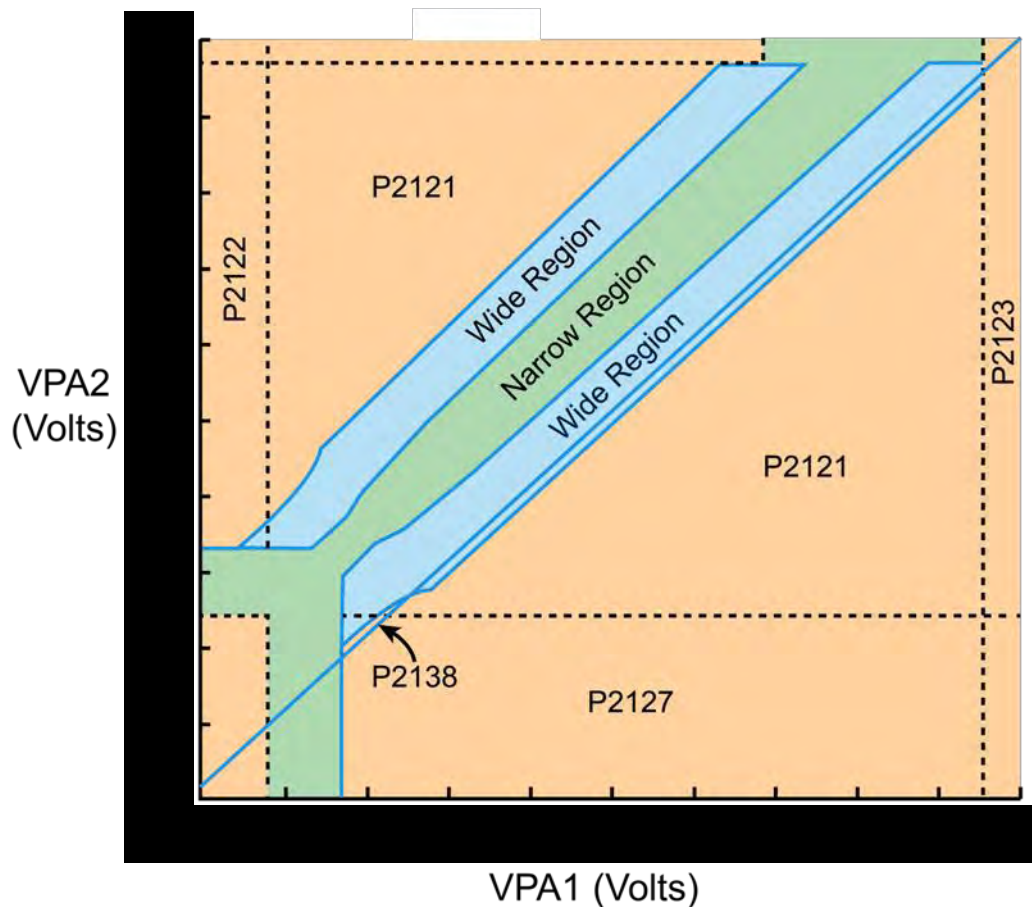


Figure 58. “Narrow” and “wide” regions of operation (2007 and later Camry vehicles).

The vehicle response on a subsequent drive cycle (ignition on/off cycle) depends upon the resistive fault VPA1 and VPA2 (i.e. where the two fall in Figure 58).

- If the fault disappears, VPA1 and VPA2 return to the narrow region when the ignition is turned on
 - The vehicle operates as normal
 - The MIL turns off after three drive cycles

- The DTC continues to be stored in memory and can be read using a diagnostic tool.
- If the resistive fault causes VPA1 and VPA2 to be outside the wide region (section 4.5) and remains in this region on pedal depression
 - The vehicle does not respond and cannot be driven when the ignition is turned back on (i.e. a dead pedal)
 - The MIL stays on
 - The DTC continues to be stored in memory and can be read using a diagnostic tool.
- If the fault causes VPA1 and VPA2 to be outside the ‘narrow’ operating region but inside the ‘wide’ operating region
 - The vehicle operates as normal once the ignition is turned back on
 - The MIL turns off after three drive cycles
 - The DTC continues to be stored in memory and can be read using a diagnostic tool.
- If the fault is such that VPA1 and VPA2 are outside both the ‘narrow’ and ‘wide’ operating regions (see Figure 58) but enter the wide operating region with pedal depression:
 - The vehicle response depends on the rate of pedal depression once the ignition is turned on
 - If the pedal is depressed quickly, the vehicle operates in the power limit mode (approximately 15° maximum opening angle)⁵⁶

⁵⁶ In addition with the vehicle in this mode, depressing the brake pedal causes the throttle request to return to 0°, regardless of the pedal request.

- If the pedal is depressed slowly, the vehicle enters a ‘non-linear’ mode of operation where the vehicle does not respond to pedal depression until the pedal depression increases a certain amount⁵⁷
- The MIL turns off after three drive cycles
- The DTC continues to be stored in memory and can be read using a diagnostic tool.

4.8.1 Non-linear Mode of Operation

The non-linear mode of vehicle operation results in a situation where the vehicle exhibits a lag in responding to pedal depression. This lag may be perceived by some drivers as a form of unintended acceleration. However, in this mode of operation, the throttle opening does not exceed the request from the pedal. The throttle response is only delayed until the vehicle exits the idle mode, but at no point does it exceed the pedal request. In addition, in this mode of operation, the throttle returns to the idle position when the pedal is released.

The non-linear mode of operation described previously occurs on slow pedal depression when the resistive fault results in VPA1 and VPA2 fall outside the wide region at idle, but enter the wide region of operation upon pedal depression⁵⁸. Table 4 shows the pedal response to resistive faults between VPA1 and VPA2 and indicates the following:

- For Denso Hall Effect sensor-based pedals, a resistive fault between VPA1 and VPA2 does not cause the sensor voltages to go outside the wide region of operation. Hence, the non-linear mode of operation cannot occur due to resistive faults between VPA1 and VPA2.
- For potentiometer pedals, the non-linear mode of operation can only be entered for resistances less than approximately 200 Ω between VPA1 and

⁵⁷ In this mode of operation, the throttle opening request from VPA1 is not sent to the throttle motor until the VPA2 idle flag is cleared. The resistive fault results in the VPA2 idle flag clearing after the VPA1 idle flag, leading to the non-linear behavior.

⁵⁸ This mode of operation results after DTC P2121 (or P1121) is triggered and the ignition is cycled.

VPA2. In addition, if the resistance between VPA1 and VPA2 is less than approximately 35 Ω , VPA1 and VPA2 do not enter the wide region on pedal depression and the vehicle cannot be operated (engine shuts down).

- For CTS (Hall Effect sensor) pedals, the non-linear mode of operation only occurs for resistances less than approximately 80 Ω between VPA1 and VPA2. In addition, if the resistance between VPA1 and VPA2 is less than approximately 10 Ω , VPA1 and VPA2 do not enter the wide region on pedal depression and the vehicle cannot be operated.

Table 4. Resistive faults between VPA1 and VPA2 for the three pedal types and region of operation

Pedal Type	Outside Narrow Region – Inside Wide Region	Outside Wide Region
Potentiometer	< 2000 Ω	< ~ 200 Ω
CTS	< ~ 150–200 Ω	< ~ 80 Ω
Denso	< ~ 100 Ω	N/A

The operation of the vehicle in the non-linear mode will be accompanied by:

- A DTC stored in memory
- Severe deterioration in vehicle performance
- Power-limited operation and closing of the throttle upon brake pedal depression when the accelerator pedal is depressed quickly
- A narrow range resistive fault between VPA1 and VPA2 with unmistakable evidence
- The resistance would be detectable on electrical testing

Although the non-linear mode of vehicle operation is unique, it does not lead to UA and would leave evidence of its existence, both a resistance between VPA1 and VPA2, and a DTC stored in memory. The non-linear mode of vehicle operation can explain a few select complaints about vehicle speed control (not uncontrolled acceleration but drivability concerns) in the NHTSA

VOQ database, but is not a realistic explanation for most reported incidents of unintended acceleration.

4.9 Multiple Series Resistive Faults Leading to Low Supply Voltage

The accelerator pedals have two sensors, each powered by a separate wire carrying 5 V from the same power supply mounted on the ECM.⁵⁹ This section discusses the consequences of a drop in that 5V power supply and a multiple-fault scenario where a series of resistive faults develops in both 5V power supply lines.

For the potentiometer pedal, VPA1 and VPA2 ratiometrically track the power supply voltage at the sensor inputs (section 4.6.5.1). As power supply voltage decreases, output voltages also decrease, resulting in lower-than-normal sensor voltages, and would thus not lead to UA. For the CTS pedal, VPA1 and VPA2 ratiometrically track the power supply voltage decline at the sensor inputs down to approximately 2.8 V and below approximately 2.8 Vdc, are almost identical. This triggers a DTC and transitions the vehicle to a Class 1.5 limp-home mode.

For the Denso pedal, VPA1 and VPA2 ratiometrically track the power supply voltage decline at the sensor inputs down to down to approximately 3.0 Vdc, but at approximately 2.9 Vdc, increase to the power supply voltage (section 4.6.5.1). Below approximately 2.8 Vdc, the two signals are almost identical. This unique behavior only occurs within the narrow window of 2.8 - 3.0 Vdc, when VPA1 and VPA2 increase toward the power supply voltage (Figure 55) and is explored below. Two faults are considered:

- Low voltage at both power supply terminals, VCPA and VCP2 at the pedal end, due to series resistors

⁵⁹ The first generation of ETCS-i systems had the accelerator pedal position sensors mounted on the throttle body and connected to the pedal by a cable. These sensors had two outputs, VPA1 and VPA2, but shared a common voltage supply and ground circuit. These sensors were never used on the Camry.

- Low voltage at VCPA and VCP2 due to an overload condition on the $V_c = +5$ Vdc power supply

4.9.1 Low Voltage at Both Supply Terminals at Pedal End

Exponent's investigation found that the sequence of faults required for multiple series resistive faults to occur in the field has not been observed and is unrealistic. Connectors are designed to prevent the development of resistive faults at connections. The Denso pedal circuitry is potted, preventing supply lines from degrading and leading to resistive faults. To develop a resistive fault in the wiring that does not lead to an open-circuit and is not detected by the ECM is extremely difficult and unrealistic. Faults would have to occur simultaneously on both lines and with very precise resistances to reach 2.8-3.0V, or a DTC will trigger and the vehicle will transition to the Class 1.5 limp-home mode of operation.

These multiple faults or failures must occur in a precise sequence to produce an uncommanded engine revving with no DTC, the "Top" failure event. Necessary and conditional simultaneous fault events for resistive faults in the wiring are as follows:

1. Insulation loss (or compromise) of VCPA wiring
2. Insulation loss (or compromise) of VCP2 wiring
3. Break in the VCPA copper wire
4. Precise series resistance between the two VCPA wires
5. Break in the VCP2 copper wire
6. Precise series resistance between the two VCP2 wires, which must be almost identical to the precise series resistance between the two VCPA wires
7. Faults not simultaneously introduced will trigger a DTC.

Resistive faults that develop in the connector would need to arise via a loose connection and contamination. Such fault conditions are mitigated by the connector technology employed by

Toyota, described in more detail in Section 10. To date, no such faults were detected during inspections of vehicles where drivers reported an unintended acceleration event. Further, no evidence has been found from inspections of parts collected in the field to support a resistive fault scenario at the connector.

4.9.2 Low Voltage Due to Power Supply Overload

Exponent's investigation found that in the remote possibility of the power supply voltage decreasing to the narrow window between 2.8 V and 3.0 V where VPA1 may rise to the power supply voltage prior to VPA2, other limp-home modes will be triggered.

Testing found that as the +5 Vdc power supply decreases to approximately 3.5 Vdc, the power supply IC generates a reset pulse for the Main and Sub processors, activates different fail safes, turning the engine off and preventing UA.

4.10 Summary

Exponent's analyses and testing of the circuit in the different pedal designs indicate the following:

- Accelerator pedals used by Toyota on vehicles equipped with ETCS-i technology are designed with two pedal position sensors.
- Testing found that single point resistive faults, power supply variations etc. cannot explain reported incidents of unintended acceleration and would result in no or minimal effect on engine speed, triggering of a fail-safe mode of operation with an accompanying DTC, or a non-linear pedal response that is not uncontrolled acceleration. DTCs would accompany operation in a fail-safe mode. If a fault is not detected, the net effect on engine speed is, at most, equivalent to a high idle condition.

- Evidence of multiple resistive faults has not been found on vehicles alleged to have experienced UA, field parts, and/or warranty data. To date, no pedal or wiring has been discovered by any investigator that exhibited multiple resistive faults even though such failures would leave unmistakable “fingerprints” on the physical wiring or other components of the vehicle, including witness marks (e.g., breached insulation, contamination between wires, low impedance measurements between wires and stains, or tin whiskers).

5 Throttle Body

This chapter will detail the design and performance characteristics of the throttle body assembly used on Toyota vehicles equipped with ETCS-i. The chapter will discuss:

- The throttle assembly and the operation of the throttle motor and throttle valve
- The interaction of the throttle with the ETCS-i system
- Potential failure modes of the throttle's electrical circuit (throttle circuit).

The chapter will also provide results from some of the testing performed to characterize the operation of the throttle body, its interaction with the ETCS-i system and the system response to a failure of one or more components in the throttle body. The testing detailed in this chapter is not intended to provide an exhaustive list of all tests performed on the throttle, but rather a representative sample of testing. No test conditions resulted in an operating condition that could explain the reported incidents of unintended acceleration.

5.1 Introduction

The primary components of the throttle body assembly related to the ETCS-i system are the throttle motor, the throttle valve and the two throttle position sensors that measure the throttle valve opening and transmit this information to the ECM. The throttle motor itself is mechanically coupled to the throttle valve through a gear train and controls the throttle valve angle and consequently the engine air flow rate. The throttle valve assembly also contains a spring mechanism that returns the valve to a 6° opening when motor power is removed. The ECM uses the throttle valve position information and other data to determine the optimal fuel quantity for emissions and power. The throttle valve opening angle is determined by information supplied by a number of sensors but most importantly from the driver-controlled accelerator pedal position or cruise control settings.

The earliest Toyota vehicles using ETCS-i technology had throttle body mounted-pedal position sensors with a cable connecting the pedal and position sensor. The cable had the ability to open the throttle valve, along with a motor driven by the ECM. However, this design was phased out starting with some 2001 model year vehicles. All Camrys equipped with ETCS-i technology use a cable-less system where pedal position sensors are mounted on the accelerator pedal and pedal position information is sent directly to the ECM. There are several other Toyota and Lexus models equipped with ETCS-i technology which have used only cable-less systems. The discussion in this section relates only to cable-less throttle controls, which is the predominant and current method of throttle valve control for Toyota vehicles equipped with ETCS-i technology.

The throttle motor is powered by the throttle motor driver IC located in the ECM. Pulse-width-modulated (PWM) signals from the throttle motor driver IC vary the speed and direction of rotation of the throttle motor, and hence, the position and rate of movement of the throttle valve. The duty cycle and polarity of this PWM signal is used to move the throttle valve to the desired position. The throttle motor works against a pair of mechanical springs that position the throttle valve opening angle to approximately 6° when the throttle motor is off. When the vehicle is in idle, the throttle valve is driven against one of the springs to set the throttle angle to approximately 2° to 4° . On a demand for power, the throttle motor works against the other spring to open the valve. The throttle motor can provide torque in both directions to open or close the throttle valve.

With ETCS-i technology, sensors in the throttle assembly generate an output dc voltage that conveys the throttle opening position information to the ECM. To understand potential failure modes of the throttle circuit and the consequences of such failures, it is helpful to understand the operation of the throttle control system. This chapter addresses throttle control system operation, including the throttle position sensors, and then analyzes the response of the ETCS-i system to the following failure modes:

- Sensor failure modes
 - Open-circuit failure
 - Short-circuit failure
 - Latch-up
- Calibration
- Electrical noise⁶⁰ (circuit design)
- Resistive faults
- Power supply variations
- Valve sticking/stuck throttle valve condition.

5.2 Throttle Circuit and Operation

Throttle position sensors pre-date ETCS-i technology, since earlier engine control modules used throttle position data to efficiently control the engine, but the ECMs in these earlier throttle body designs did not control the position of the throttle valve.

In Toyota vehicles equipped with ETCS-i, two electrical sensors inside the throttle assembly monitor the throttle valve opening angle and generate voltage signals, VTA1⁶¹ and VTA2, based on the valve opening angle. VTA1 provides information on the throttle valve position to the ECM. VTA2 is a monitoring signal to verify the operation of the VTA1 circuit. The sensor voltages vary between 0 V and 5 V (0.69 to 5 V for Hall Effect based throttle sensors), and are transmitted to the VTA1 and VTA2 ECM connector terminals.

Toyota vehicles equipped with ETCS-i technology have used two different sensor technologies to detect the throttle position: potentiometers and Hall Effect sensors.

⁶⁰ EMI testing is discussed in a separate Exponent report.

⁶¹ In some manuals, VTA1 is sometimes referred to as VTA.

5.2.1 Potentiometer Based Throttles

Two separate potentiometers detect throttle valve position. There are two potentiometric throttle position sensor designs as shown in Figure 59 and Figure 60. The two potentiometer wipers slide along resistive elements as the throttle valve opens, changing the voltage divider circuit resistance values and the output voltage VTA1 and VTA2 generated by that potentiometer.



Figure 59. Potentiometer-based throttle position sensor in 2002 Camry L4 engine.

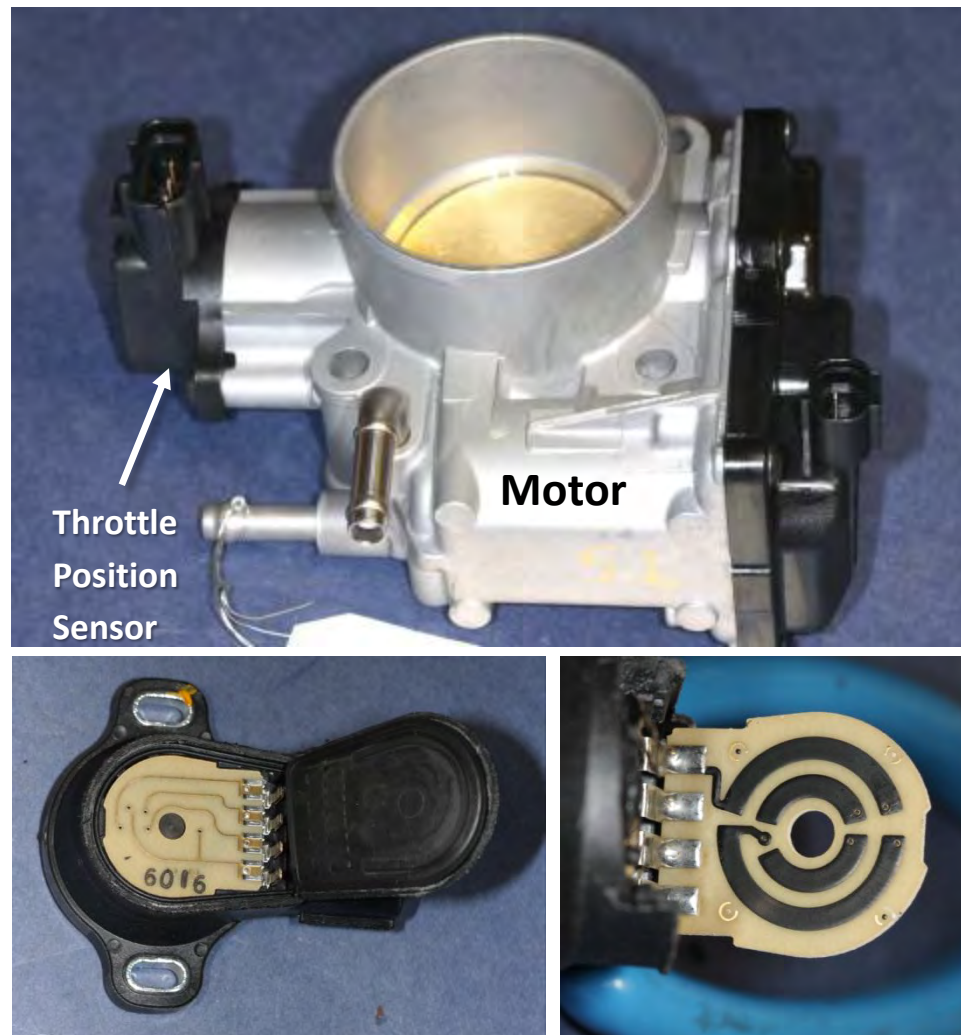


Figure 60. Throttle body for 2002 Camry V6 (top), throttle position sensor connections (lower left), potentiometers on throttle position sensor (lower right).

The two potentiometer based circuits have the following characteristics:

- VTA2 has a positive voltage offset of approximately 1.6 V as compared to VTA1 for a fully closed throttle.
- As the throttle valve opening angle increases, both signal voltages increase linearly, VTA1 over its entire range, while VTA2 reaches and remains at a voltage near 5 V for large throttle openings.

- VTA1 has a throttle opening slope of $0.04\text{V}/^\circ$, while VTA2 has a throttle opening slope of $0.05\text{V}/^\circ$.
- The throttle body is specified and tested for operation from $\blacksquare^\circ\text{C}$ to $\blacksquare^\circ\text{C}$, and for storage from $\blacksquare^\circ\text{C}$ to $\blacksquare^\circ\text{C}$. Additional tests include high humidity, vibration, chemical resistance, salt and dust exposure.
- At idle, VTA1 $\sim 0.8\text{ V}$ and VTA2 $\sim 2.5\text{ V}$.
- For a maximum throttle opening angle (84°), the voltages are: VTA1 $\sim 4\text{ V}$ and VTA2 $\sim 5\text{ V}$.

Figure 61 shows VTA1 and VTA2 as a function of the potentiometer angle.

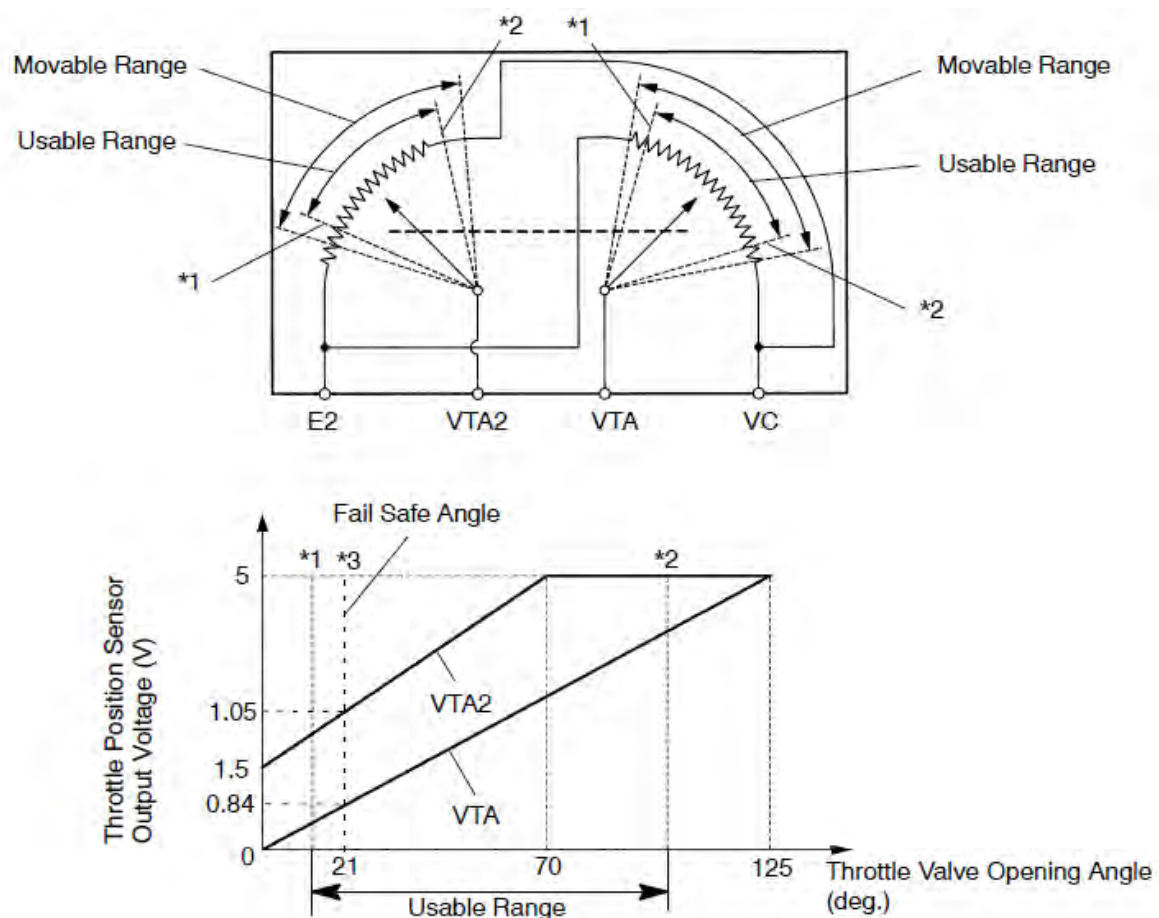


Figure 61. Potentiometer based throttle circuit response. X-axis angles refer to angles along the perimeter of the potentiometer (drawing on the left), not the throttle angle, which is approximately 10° smaller.

5.2.2 Hall Effect Sensors

The potentiometer sensors were replaced, in later model years, by Hall Effect sensors. Figure 62 - Figure 64 shows the components of a throttle body with Hall Effect throttle position sensors. The throttle valve (blue arrow) is coupled to a gear train (red arrows) and is driven by the throttle motor (green arrow). The throttle motor is powered by the throttle motor driver IC located in the ECM.

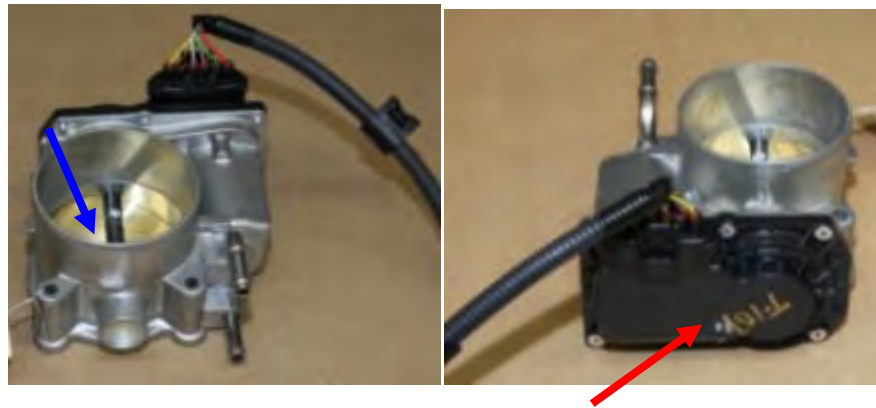


Figure 62. Throttle body of a 2007 Toyota V6 Camry showing the throttle valve (blue arrow) and gear housing (red arrow).

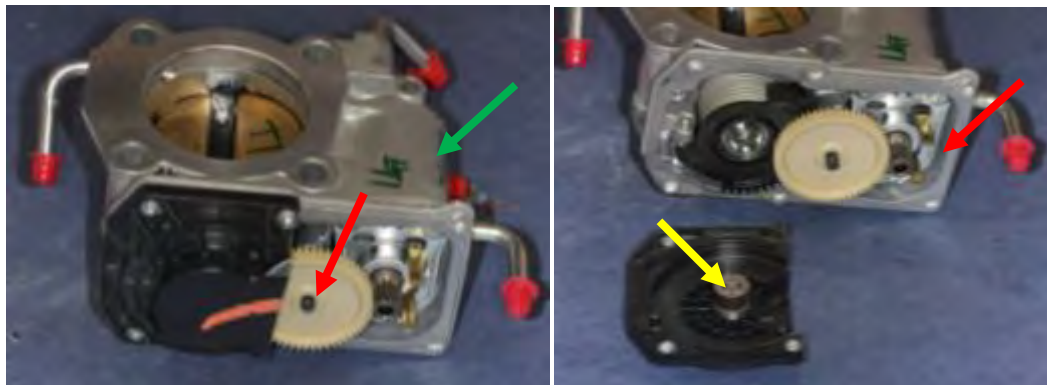


Figure 63. 2007 Toyota L4 Camry gear housing sectioned to show the gearing (red arrow): Hall Effect sensors (yellow arrow), and throttle motor housing (green arrow).



Figure 64. Gear housing sectioned to show the gears coupled to the throttle motor. Permanent magnets which provide the magnetic field sensed by the Hall Effect sensors are shown by the blue arrow.

Hall Effect sensor-based throttles have the following characteristics:

- When the current to the motor is cut (such as during fail-safe operation), the throttle valve returns to a position of approximately 6°
- VTA1 has linear voltage increase with the throttle angle
- At idle, VTA2 is offset approximately 1.5 V compared to VTA1.

Figure 65 is a block diagram of the Hall Effect sensor-based throttle and the output voltage characteristics of the throttle circuit as a function of the throttle valve opening angle.

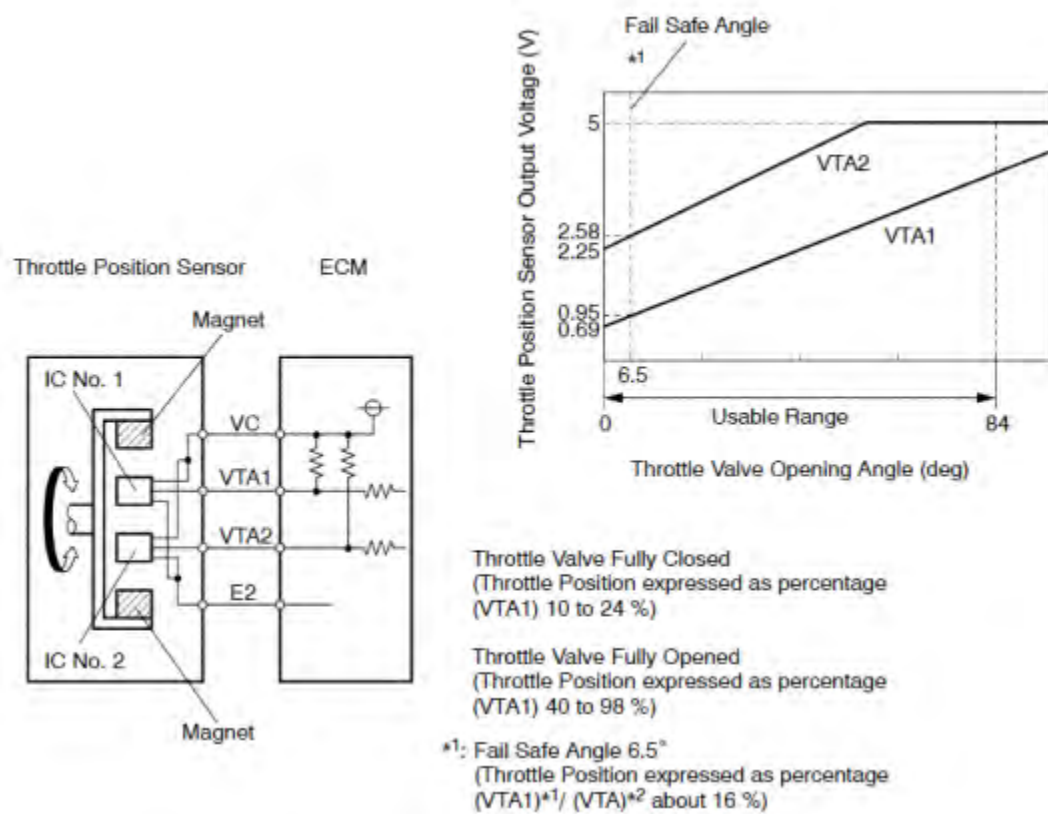


Figure 65. Hall Effect sensor output characteristics.

The Hall Effect throttle position sensors have the following characteristics:

- The throttle body has two Hall Effect sensors in physically independent packages
- The Hall Effect sensors have on-board decoupling capacitors for noise immunity
- On-board capacitors are used to provide increased noise immunity at each of the throttle position sensor output terminals
- At the ECM, each of the output signals is pi-filtered
- Pull-up resistors are also used at the outputs to provide protection against open circuit failures.

5.2.3 Characterization Tests

A series of tests were performed to characterize the operation of the throttle circuit.

5.2.3.1 Throttle Motor Voltage and Current Waveforms

The throttle motor voltage and current waveforms for a 2005 Toyota Camry with a 2.4 L engine at idle are shown in Figure 66.

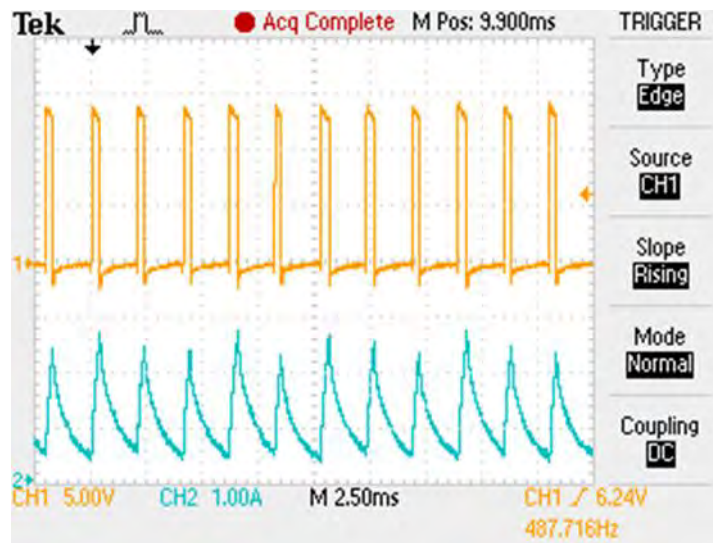
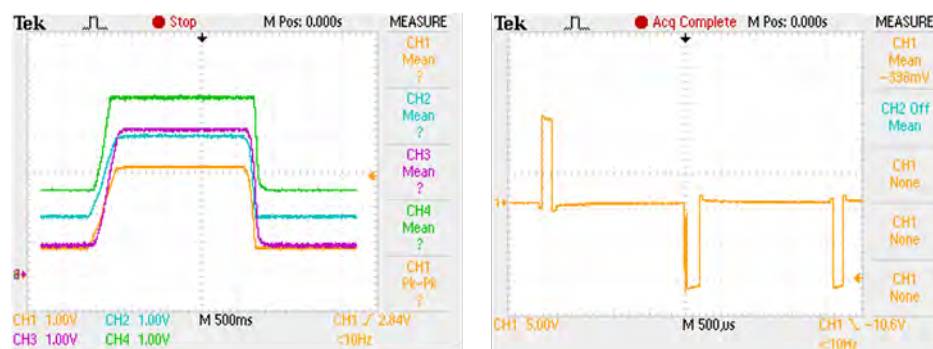


Figure 66. Throttle motor voltage and current. Engine at idle. The feedback loop adjusts the duty cycle in real-time.

The throttle motor voltage (yellow) and current waveforms (blue) appear as expected for this type of PWM controller, where the feedback loop adjusts the duty cycle in real-time.

5.2.3.2 Comparison of Pedal and Throttle Signal Waveforms

In-vehicle tests were conducted to characterize and compare the pedal and throttle sensor output voltage waveforms and the throttle motor voltage waveforms with the accelerator pedal in different positions. Figure 67 shows the test waveforms for a 2007 Camry L4 using a CTS pedal.



Left image waveforms: Ch 1: VPA1, Ch 2: VPA2, Ch 3: VTA1, Ch 4: VTA2; 1 V/div., 500 ms./div.
 Right image waveforms: Voltage waveform of throttle motor: 5 V/div, 500 µs/div.

Figure 67. Test Condition #3: Engine ON, accelerator pedal in different positions.

The two pedal outputs (VPA1 and VPA2) and the two throttle position sensor circuit outputs (VTA1 and VTA2) track each other. These test results also confirmed the results from the Hardware-in-the-Loop simulation performed for a 2007 V6 Camry (section 7.9).

5.3 Throttle-Body Related Fail-Safes

Checks are performed to monitor the status of the throttle motor and the throttle position sensors to ensure that the system operates as designed. Two independent Hall Effect sensors in the throttle motor assembly monitor the throttle valve opening angle and transmit this information to the ECM. The two throttle position sensors each output a voltage (VTA1 and VTA2) with a magnitude between 0 V and 5 V (between 0.7 V and 5 V for Hall Effect sensor-based throttle assemblies) where the output voltage indicates the amount of throttle valve opening. When the vehicle is at idle, VTA1 has a positive offset of approximately 0.7 V with respect to ground and VTA2 has a positive offset of approximately 2.3 V with respect to ground. The ECM monitors data from both throttle position sensors and sets a diagnostic trouble code (DTC) if the sensor outputs are outside a pre-set range, indicating that there is a fault with the throttle position sensor circuit. A number of fault conditions (e.g. open-circuit fault, a short-circuit fault, etc.) could cause the throttle position sensor output signals to deviate from their expected values. These faults are detected by the ECM, which transitions the vehicle to either the “fail-safe” mode or causes the vehicle to shut down.

The condition of the throttle motor is also monitored by measuring its current draw and the pulse width modulated signal used to drive it. If these signals are not within expected ranges, a DTC is triggered and the vehicle transitions to the fail-safe mode. Table 5 summarizes the throttle motor related DTCs. The logic and fault conditions that trigger a DTC in other Camry model year vehicles are almost identical. The slight deviations are due to requirements mandated by the California Air Resources Board (CARB), which led to a few fault condition threshold value changes.

Table 5. DTC associated with throttle body related faults

DTC 2002 Camry	DTC 2003–2009 Camry	Description ⁶²	Fault Condition
P0120	P0120	Throttle / Pedal Position Sensor / Switch "A" Circuit Malfunction	VTA1 Intermittent Open/Short
P0121	P0121	Throttle / Pedal Position Sensor / Switch "A" Circuit Range/Performance Problem	Difference between VTA1 and VTA2
P0120	P0122	Throttle/Pedal Position Sensor /Switch "A" Circuit Low Input	VTA1 short/low
P0120	P0123	Throttle/Pedal Position Sensor /Switch "A" Circuit High Input	VTA1 high fault
P0120	P0220	Throttle/Pedal Position Sensor /Switch "B" Circuit	VTA2 Intermittent Open/Short
P0120	P0222	Throttle/Pedal Position Sensor /Switch "B" Circuit Low Input	VTA2 short/low
P0120	P0223	Throttle/Pedal Position Sensor /Switch "B" Circuit High Input	VTA2 high fault
P0120	P2135	Throttle/Pedal Position Sensor/Switch "A"/"B" Voltage Correlation	Short between VTA1 and VTA2 circuits
P1125	P2102	Throttle Actuator Control Motor Circuit Low	Open-circuit fault in throttle actuator circuit
P1125	P2103	Throttle Actuator Control Motor Circuit High	Short-circuit fault in throttle actuator circuit
P1128	P2111	Throttle Actuator Control System - Stuck Open	Throttle stuck open
P1128	P2112	Throttle Actuator Control System - Stuck Closed	Throttle stuck closed
P1127	P2118	Throttle Actuator Control Motor Current Range / Performance	Throttle control system power source open circuit
P1129	P2119	Throttle Actuator Control Throttle Body Range / Performance	Throttle opening angle variation and deviation

⁶² The description of the DTC on the table is for the 2003 – 2009 Camry. The descriptions of the DTC for the 2002 Camry are different in a few places.

The fault detection scheme for the throttle position sensors monitors the VTA1 and VTA2 signals to ensure that they are in an acceptable range⁶³. In addition to monitoring the absolute values of VTA1 and VTA2, the relative difference is also monitored. A DTC is triggered if the difference is too small or too large. The allowable deviation at any time is dependent upon the throttle valve opening angle and is smallest at idle when the throttle valve opening angle is minimal.

5.4 Throttle Position Learning

The throttle position learning is similar to the learning performed for the pedal position after ignition on. The initial throttle valve position is “learned” by the software after ignition on⁶⁴ and these learned values are used by the software system to calculate the desired throttle valve opening angle. If these values are outside a specific range at start up, then default values are used for processing, and in most cases a DTC is triggered. If a DTC is triggered due to the throttle related diagnostics, the learned values are not over-written. The final throttle valve position depends on the learned position, the request from the idle speed control (ISC) module and the driver request (through the pedal or the cruise control system).

5.5 Throttle Circuit Failure Modes

The Main processor monitors the throttle position sensor signals to detect any deviation. Faults (e.g. short-circuit between the sensor signal outputs or an open-circuit failure) transition the vehicle to a fail-safe mode. The Sub processor on the ECM provides independent monitoring of the throttle circuit and also can transition the vehicle to the fail-safe mode upon detecting a fault.

⁶³ Faults are triggered if the absolute values of the output of the two independent throttle circuits fall outside the acceptable values or if the relationship between the two circuit output signals deviates from the designed relationship. In addition, the ETCS-i is also designed to perform a calibration check each time the vehicle's ignition is turned on.

⁶⁴ A spring in the throttle assembly keeps the valve at 6° when the throttle valve is not powered. When the vehicle is at idle, the throttle valve is closed against this spring to be at an opening of approximately 2° to 4°.

5.5.1 Sensor Failure Modes

The ETCS-i system is designed to detect a failure (short-circuit, open-circuit etc.) of one or both sensors in the throttle assembly. These throttle related fail-safes are discussed in detail in section 5.3. A latch-up of the Hall Effect sensors may also cause the throttle position sensor output signals to deviate from their normal operating values. In the event of a latch-up of one or both Hall Effect sensors, numerous software fail-safes will detect this condition and transition the vehicle to a fail-safe mode. Table 6 summarizes the various possible scenarios for latch-up on the throttle circuit.

Table 6. Vehicle response to a latch-up of the Hall Effect sensors in the throttle circuit

Circuit	Circuit Condition due to Latch-up	Vehicle Response
VTA1 ⁶⁵	High	If VTA1 rises to the power supply voltage (+5 Vdc), DTC P0123 will be triggered and the vehicle will transition to the fail-safe mode.
	Low	If VTA1 drops to ground, DTC P0122 will be triggered and the vehicle will transition to the fail-safe mode.
	Intermediate	If VTA1 doesn't trigger DTC P0122 or DTC P0123, then DTC P0121 will be triggered if the difference between VTA1 and VTA2 exceeds the allowable range. If DTC P0121 is not triggered and VTA1 cannot respond to throttle valve opening angle changes, the ECM will detect a "throttle stuck open," triggering DTC P2111 (throttle stuck open) or DTC P2112 (throttle stuck closed).
VTA2 ⁶⁶	High	If VTA2 rises to the power supply voltage (+5 Vdc), DTC P0223 will be triggered and the vehicle will transition to the fail-safe mode.
	Low	If VTA2 drops to ground, DTC P0222 will be triggered and the vehicle will transition to the fail-safe mode.
	Intermediate	If VTA2 doesn't trigger DTC P0222 or DTC P0223, then DTC P0121 will be triggered if the difference between VTA1 and VTA2 exceeds the allowable range. The ECM uses VTA1 to monitor the throttle valve opening angle and VTA2 to monitor VTA1. Hence, a latch-up of VTA2 that does not trigger a DTC, does not affect the throttle opening angle and the vehicle will continue normal operation. If both sensors latch-up and rise to the power supply line or fall to the ground line then numerous DTCs (as discussed in the preceding two bullets) will be triggered transitioning the vehicle to the fail-safe mode.
VTA1 & VTA2		The latch-up condition will prevent the value of the VTA1 signal from responding to changes in the throttle valve opening angle. This will be detected as a stuck-throttle condition which will trigger DTC P2111 (throttle stuck open) or DTC P2112 (throttle stuck closed). Based on the analysis above, latch-up conditions affecting both the VTA1 and VTA2 signals at the same time and resulting in acceleration without triggering any DTCs or activating any fail-safe mechanisms are not realistic and are not consistent with the reported incidents of unintended acceleration.

⁶⁵ If the latch-up condition occurs in a manner that does not affect the operation of the VTA1 signal, then the vehicle continues to operate as normal.

⁶⁶ If the latch-up condition does not affect VTA2, then normal vehicle operation continues.

5.5.2 Calibration

Hall Effect ICs compensate for temperature variations. In addition, the software system is self-calibrating through the throttle position learning process.⁶⁷ A DTC is triggered if the “learned” values are outside certain thresholds (section 5.4).

5.5.3 Electrical Noise

Potentiometer Based Throttle Position Sensor—The potentiometer throttle position sensor is a passive resistive element, and does not rely on external protection elements. There are no other passive or active components in the circuit of the sensor to couple electrical noise. Several design features incorporated in the ECM provide protection against electrical noise as discussed in section 6.5.

Hall Effect Sensor-Based Throttle Position Sensor—The two Hall Effect sensors use active circuits for generating output voltages. Each Hall Effect throttle position sensor has a decoupling capacitor on the power supply line and a filter capacitor on its output terminal. EMI testing performed by Exponent is detailed in a separate Exponent report. No cause for the reported incidents of unintended acceleration was found in this testing.

5.5.4 Resistive Faults

Contaminants and/or tin whiskers (Appendix G) can lead to a resistive fault between the various signals on the throttle circuits. Several throttle design features provide protection against contaminants.

Potentiometer Based Throttle—The throttle position sensors are packaged in a closed plastic housing to minimize the likelihood of moisture and contaminants coming in contact with the sensor assembly.

⁶⁷ Learned values are updated at ignition on only under certain conditions.

Hall Effect Sensor Based Throttle—The Hall Effect sensor-based throttle assembly is similar to the Denso pedal assembly (including the ICs and the filter capacitors). The electrical circuit is sealed and potted, protecting against moisture, contaminants and resistive faults.

5.5.4.1 Tin Whiskers

Camry throttle body electronics employ potentiometers for 2002-2003 model years and Hall Effect sensors for 2004-2010 model years. Camry potentiometer sensors do not use tin platings, so are not susceptible to tin whisker shorting. The Hall Effect sensors are potted and not susceptible to tin whisker-induced shorting.

5.5.4.2 Resistive Fault Testing Performed

Resistive faults on the throttle circuit may result in a deviation in the throttle position sensor output signals. The effects of resistive faults between any pair of the five output terminals on the throttle assembly connector or in series with any of the five output terminals were considered. Figure 68 depicts five types of resistive faults which have the potential of changing the throttle position sensor output signals and affecting vehicle operation.

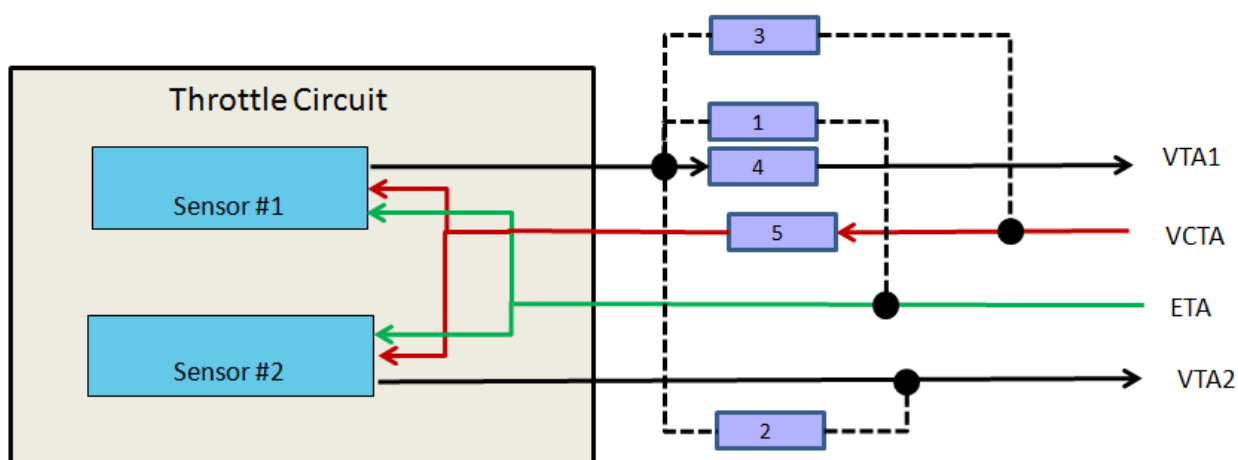


Figure 68. Single point resistive fault conditions that affect throttle position sensor output.⁶⁸

⁶⁸ Many of the depicted fault conditions are impractical requiring the compromise of multiple layers of protection to achieve the fault. Selected scenarios are considered in this section of the report for completeness.

The five resistive faults depicted in Figure 68 are:

1. Output to Ground: VTA1 (or VTA2) to ETA
2. Output to Output: VTA1 to VTA2
3. Output to +5 Vdc: VTA1 (or VTA2) to VCTA
4. Series resistance on output (VTA1)
5. Series resistance on +5 Vdc (VCTA).

The subsequent sections describe the vehicle response to simulated resistive faults for various throttle types.

5.5.4.3 Resistive Fault between Output and Power Supply Ground Terminal (Fault 1)

Potentiometer Based Throttles—Figure 69 shows the response of the throttle valve to a resistive fault between VTA1 and ground (ETA).

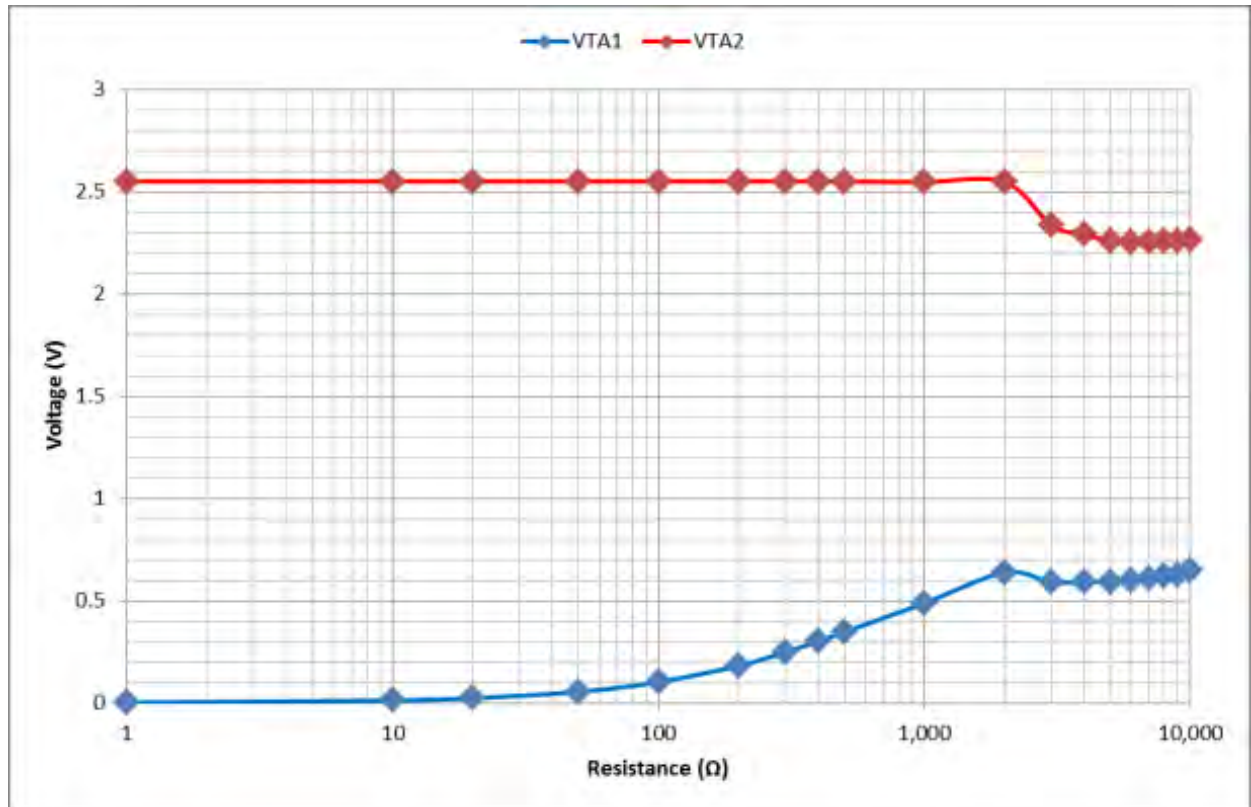


Figure 69. Throttle position sensor output voltages as a function of a fault resistance between VTA1 and the ground terminal for a potentiometer-based throttle position sensor.

Testing (2002 V6 Camry at idle) demonstrated:

- No change in throttle opening angle and VTA1 for resistance values greater than approximately 10 kΩ
- VTA1 started to drop for resistance below approximately 10 kΩ. This resulted in a small increase in engine rpm (increase from approximately 600 rpm to approximately 1000 rpm)

- DTCs (P0120 and P0121) were set for resistance values of less than approximately 2 k Ω . These transitioned the vehicle to the fail-safe mode.

Although a small rise in the throttle valve opening angle and engine rpm was observed for a limited range of resistance values (2 k Ω to 10 k Ω), this rise is limited and cannot explain the reported incidents of unintended accelerations. No evidence has been found of such resistive faults developing.

Hall Effect Sensor Based Throttles—Figure 70 shows the response of the throttle valve for a resistive fault between VTA1 and ground (ETA).

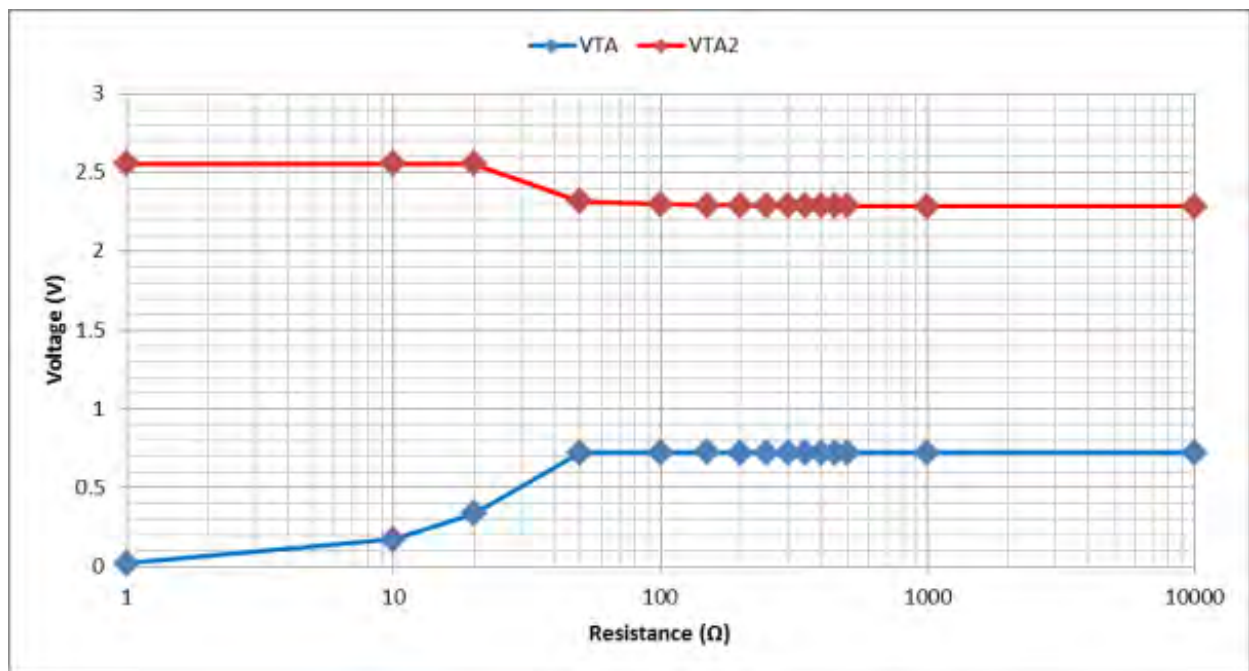


Figure 70. Throttle position sensor output voltage as a function of a fault resistance between VTA1 and the ground terminal for a Hall Effect throttle position sensor.

Testing (2007 V6 Camry at idle) demonstrated:

- No measurable change in the throttle opening angle and VTA1 was observed for resistance values greater than approximately 50 Ω .
- Below approximately 50 Ω , VTA1 starts to decrease. A corresponding rise in the throttle valve opening angle and engine rpm was observed as the ECM

compensated for the decrease in VTA1. A small increase in engine rpm from approximately 800 rpm to approximately 1000 rpm was observed.

- DTCs (P0121 and P0122) were set for resistance values of less than approximately 20 Ω . These transitioned the vehicle to the fail-safe mode.

Although a small rise in the throttle valve opening angle and engine rpm was observed for a limited range of resistance values (20 Ω to 50 Ω), this rise is limited and cannot explain the reported incidents of unintended accelerations. No evidence has been found of such resistive faults developing.

5.5.4.4 Resistive Faults between VTA1 and VTA2 (Fault 2)

Electrical testing was conducted to determine the throttle response to resistive faults between the throttle sensor outputs, VTA1 and VTA2. The response of each throttle type will be discussed individually. **Potentiometer Based Throttle**—Figure 71 shows the response of the throttle to a resistive fault between VTA1 and VTA2.

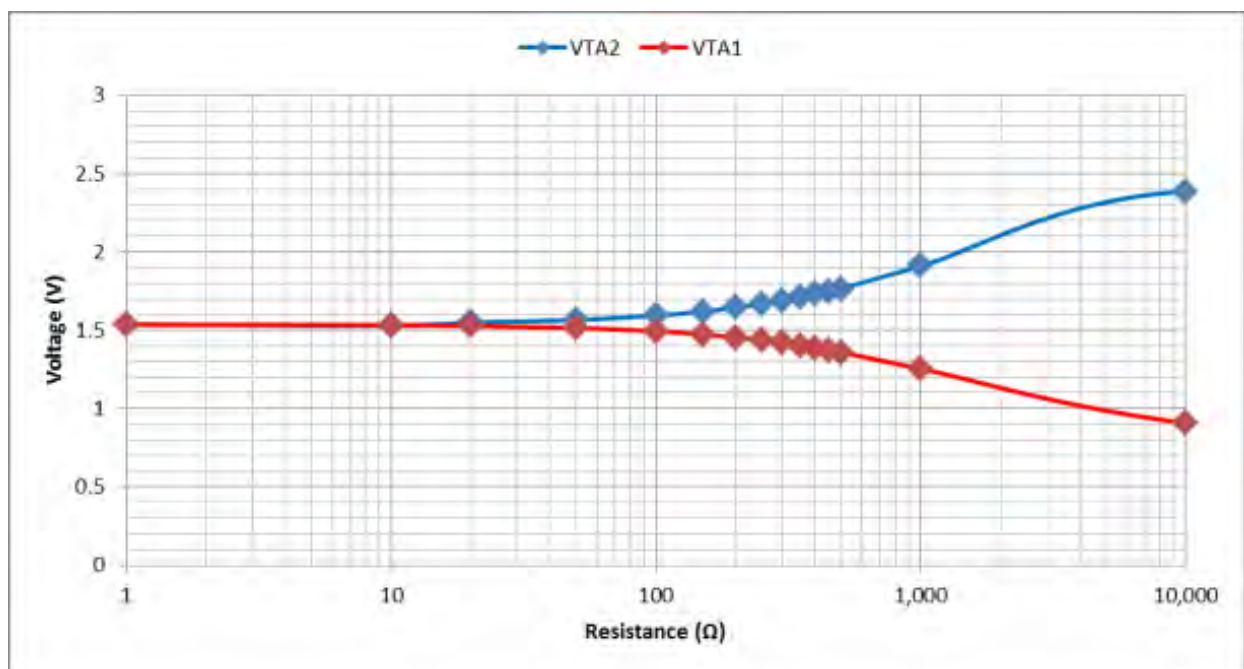


Figure 71. Resistive fault between VTA1 and VTA2 for a potentiometer based throttle.

Testing (2002 V6 Camry at idle) demonstrated:

- A DTC (P0121) was set for resistance values of less than approximately 10 k Ω and the vehicle's engine shut down
- No change in engine rpm occurred for resistance values greater than 10 k Ω
- No resistance value was identified that could lead to UA due to a resistive fault between VTA1 and VTA2.

Hall Effect Sensor Based Throttle—Figure 72 shows the response of the throttle to a resistive fault between VTA1 and VTA2.

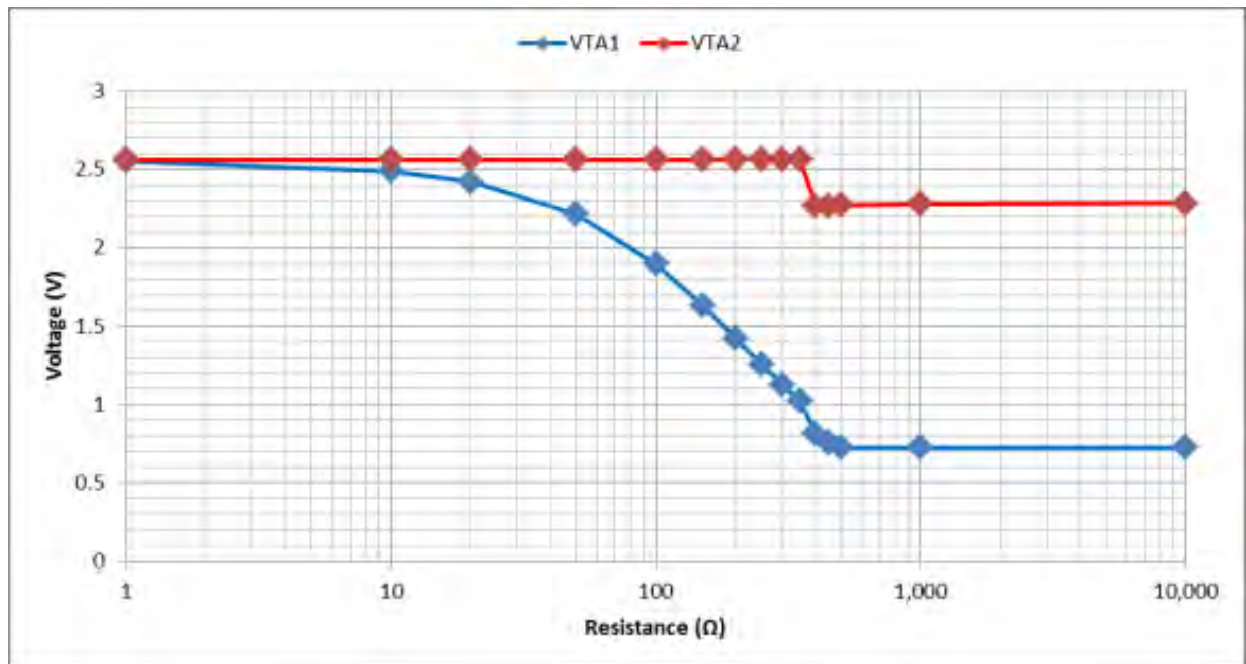


Figure 72. Resistive fault between VTA1 and VTA2 for a Hall Effect sensor based throttle.

Testing (2007 V6 Camry at idle) indicated that:

- Engine rpm decreased as the resistance was decreased from 1 M Ω to 350 Ω
- A DTC (P2111) was set for resistance value of approximately 350 Ω and the vehicle's engine shut down.

No resistance value was identified that could lead to UA due to a resistive fault between VTA1 and VTA2.

5.5.4.5 Resistive Fault between Output and Power Supply Terminals (Fault 3)

Potentiometer Based Throttle Assembly—Figure 73 shows the response of the throttle valve to a resistive fault between VTA1 and the +5 Vdc terminal.

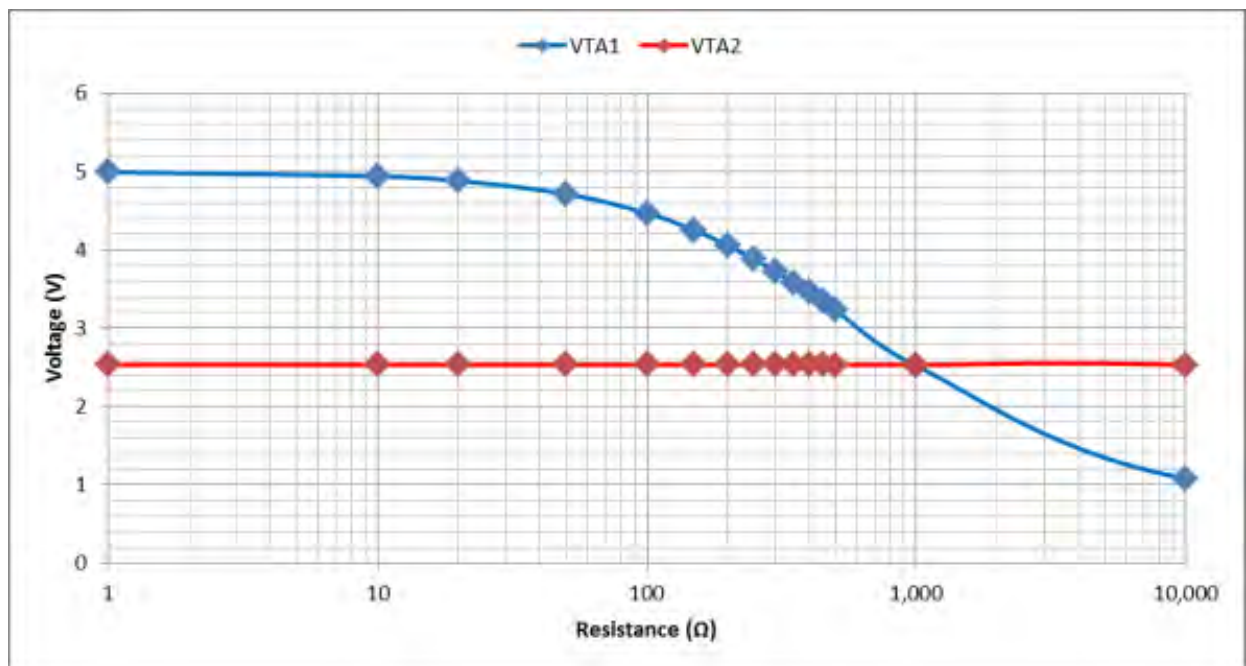


Figure 73. Throttle position sensor output voltages as a function of a fault resistance between VTA1 and the +5 Vdc terminal for a potentiometer based throttle position sensor.

Testing (2002 V6 Camry at idle) demonstrated:

- For a resistive fault of less than approximately 10 kΩ, VTA1 started to rise to the power supply voltage, causing the ECM to compensate by closing the throttle valve.

- Testing on a 2002 V6 Camry indicated that a DTC (P0121) would be triggered for resistances less than approximately 10 k Ω which would transition the vehicle to the fail-safe mode.

Hall Effect Sensor Based Throttles—Figure 74 illustrates the throttle valve response to a resistive fault between VTA1 and the +5 Vdc terminal.

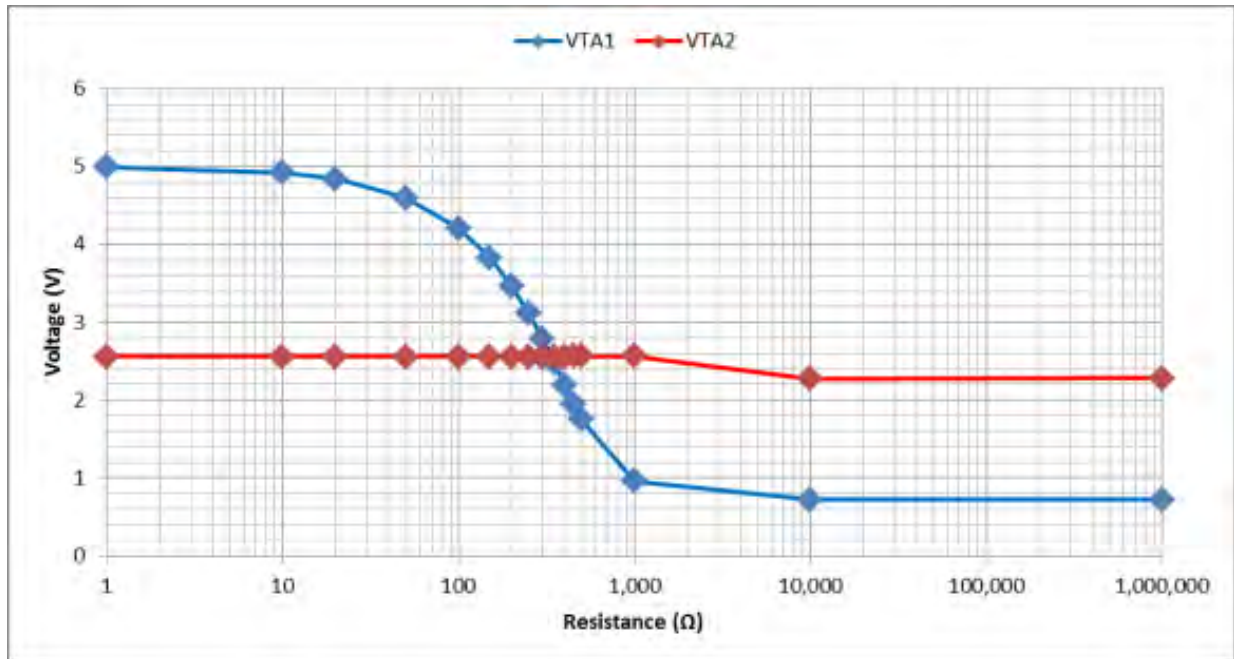


Figure 74. Throttle position sensor output voltage as a function of a fault resistance between VTA1 and the +5 Vdc terminal for a Hall Effect throttle position sensor.

Testing (2007 V6 Camry in idle) demonstrated:

- For a resistive fault of less than approximately 10 k Ω ⁶⁹, VTA1 started to rise to the power supply voltage, causing the ECM to compensate by closing the throttle valve.
- Testing on a 2007 V6 Camry indicated that a DTC (P0121) would be triggered for resistances less than approximately 1 k Ω , which would transition the vehicle to the fail-safe mode.

⁶⁹ Minimal change in the throttle opening angle will occur as the resistance is dropped from 10 k Ω to 1 k Ω .

5.5.4.6 Series Resistance in VTA1 Circuit Output (Fault 4)

Testing was performed to characterize the ETCS-i system response to a resistive fault at the output of the VTA1 circuit between the VTA1 terminal at the throttle end and the VTA1 terminal at the ECM end.

Potentiometer Based Throttle—Figure 75 shows the response of the throttle to a resistive fault in between the VTA1 output terminal on the throttle and the VTA1 input terminal on the ECM.

Testing demonstrated that:

- There was minimal change in VTA1 at the throttle circuit (actual throttle valve opening angle) until the series resistance increased to above approximately 10 k Ω . In addition, minimal change in engine RPM was observed for resistance values of less than 10 k Ω .
- A DTC (P0121) was set and the vehicle transitioned to the fail-safe mode for series resistance values greater than 10 k Ω .
- At 1 M Ω , the engine rpm increased to 1500 rpm momentarily, triggering DTC P0121 and transitioning the vehicle to the fail-safe mode.
- No series resistive fault was identified which could cause an increase in engine rpm without triggering a DTC.

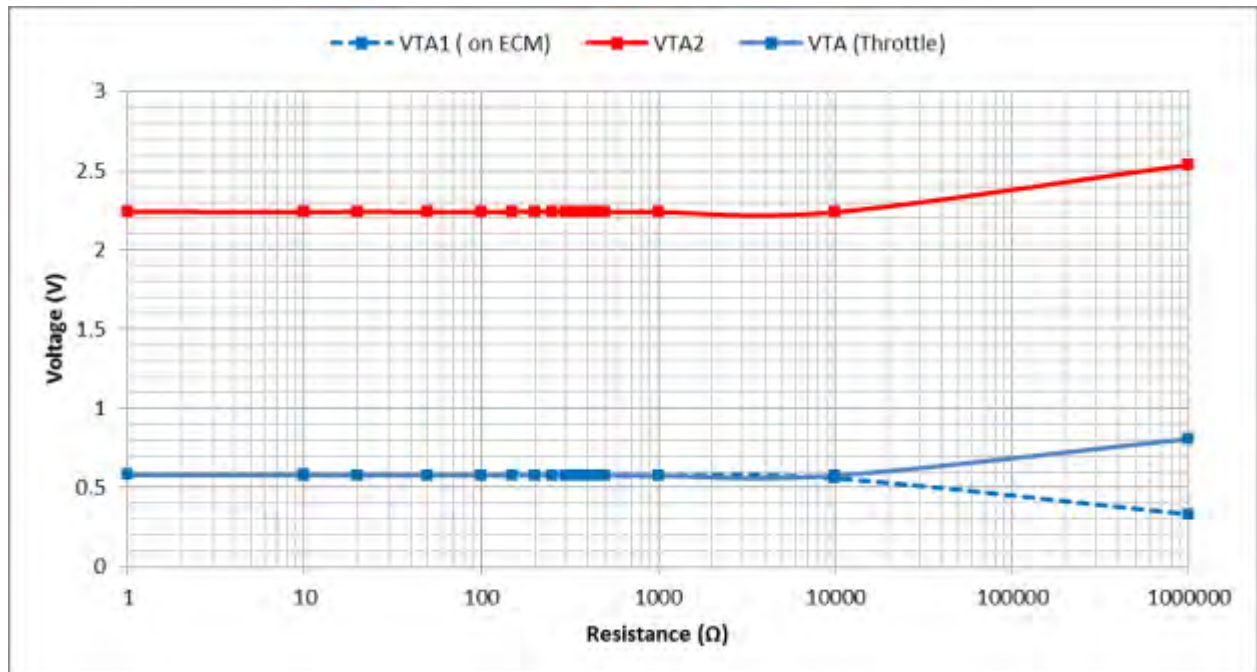


Figure 75. Resistive fault in series with the VTA1 signal between the throttle circuit and the ECM for a potentiometer based throttle position sensor.

Hall Effect Sensor Based Throttle—Figure 76 shows the response of the Hall Effect sensor-based throttle in a 2007 V6 Camry (at idle) to a resistive fault between the throttle VTA1 output terminal and the ECM VTA1 input terminal. Testing demonstrated that:

- There was minimal change in VTA1 at the throttle circuit (actual throttle valve opening angle) until the series resistance increased to above approximately 10 kΩ. In addition, minimal change in engine RPM was observed for resistance values of less than 10 kΩ.
- A DTC (P0121) was set and the vehicle transitioned to the fail-safe mode for series resistance values greater than 10 kΩ.
- For a resistive fault of approximately 10 kΩ, a small increase in engine rpm to 1200 rpm was observed. However, this was followed by the triggering of a DTC (P0121).
- No series resistive fault was identified which could cause an increase in engine rpm without triggering a DTC.

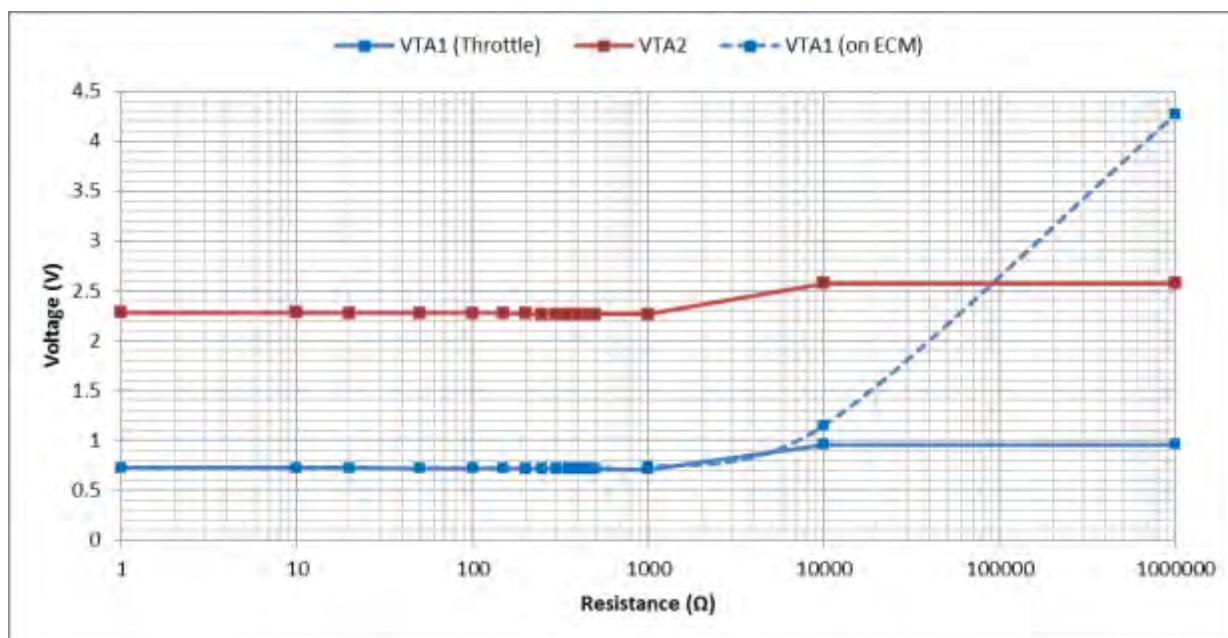


Figure 76. Resistive fault in series with the VTA1 signal between the throttle circuit and the ECM for a Hall Effect sensor based throttle position sensor.

5.5.4.7 Series Resistance on VCTA Circuit (Fault 5)

The VCTA terminal provides the dc power to the throttle position sensors. A resistance in series with the VCTA input will cause a drop in the power supply voltage to the potentiometer/Hall Effect sensors. Testing was conducted to determine the throttle response to series resistive faults on the VCTA circuit. The response of each throttle type will be discussed individually.

Potentiometer Based Throttle—Figure 77 shows the response of the throttle to this simulated fault condition.

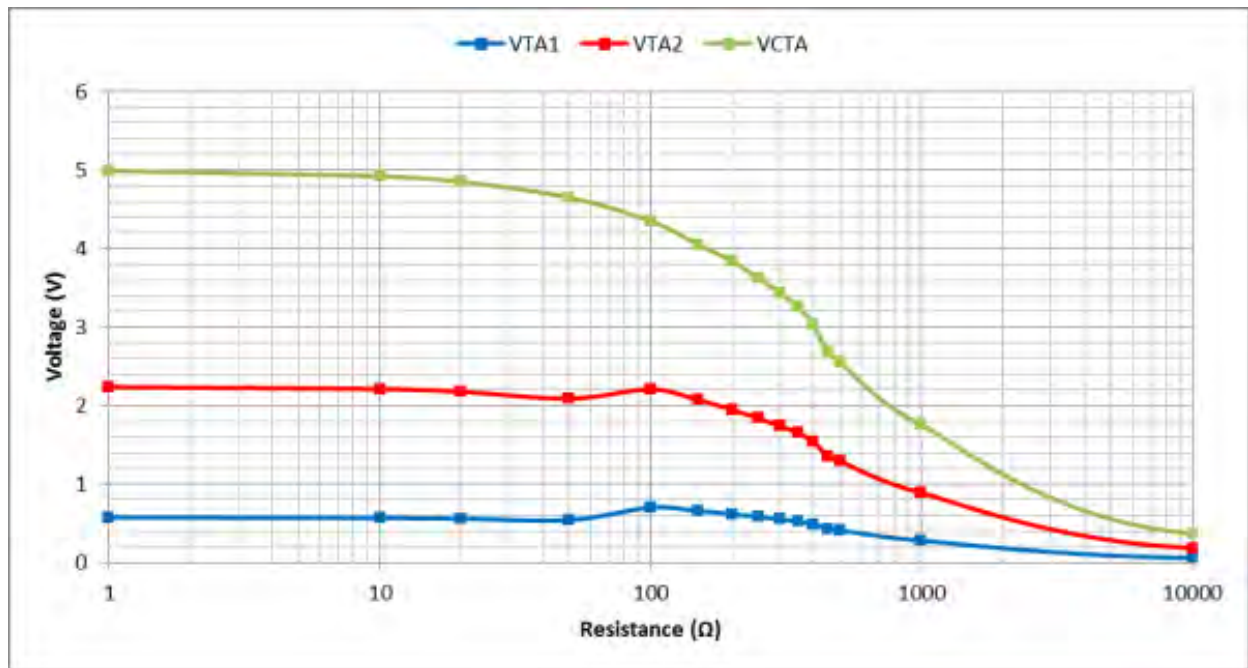


Figure 77. Potentiometer based throttle output as a function of series resistance on the VCTA line.

Testing (on a 2002 V6 Camry at idle) demonstrated that:

- The supply voltage for the circuit generating VTA1 and VTA2 drops due to a series resistance fault. Since the potentiometer sensors are ratiometric, a drop in the supply voltage to the sensors results in a drop in VTA1 and VTA2. The algorithm in the ECM compensates by opening the throttle further. This was observed during testing. For resistances up to 20 Ω, there was no change in engine rpm (610 rpm). At approximately 50 Ω, the engine rpm at idle increased to approximately 650 rpm. At 100 Ω, the engine rpm rose to approximately 1,500 RPM, and a DTC (P0121) was set, resulting in the vehicle transitioning to the fail-safe mode.

- Even though a minimal rise in engine RPM resulted due to the introduced series fault, the fail-safes operated to prevent a higher rise in engine rpm and a greater opening of the throttle valve angle.

Hall Effect Sensor Based Throttles—Figure 78 shows the response of the throttle to the simulated fault condition.

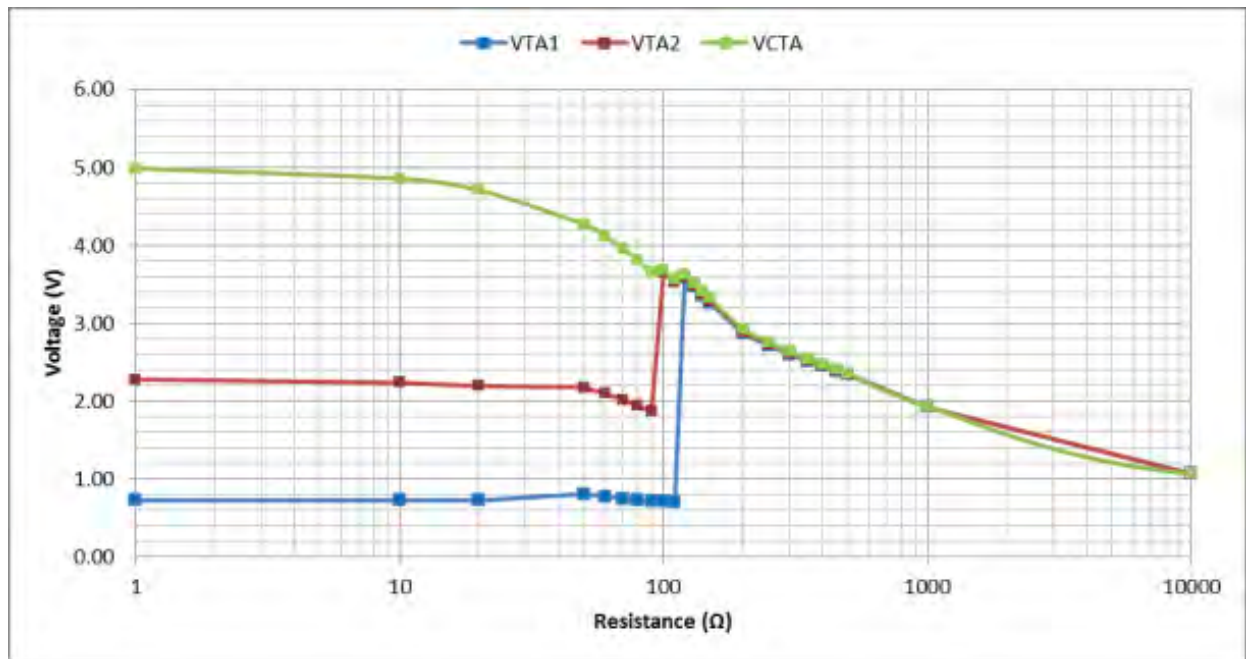


Figure 78. Hall Effect sensor based throttle output as a function of resistance in series with the power supply voltage signals (VCTA).

Testing (2007 V6 Camry at idle) indicated the following:

- The supply voltage for the circuit generating VTA1 and VTA2 drops due to a series resistance fault. Since the Hall Effect sensors are ratiometric, a drop in the supply voltage to the sensors results in a drop in VTA1 and VTA2. The algorithm in the ECM compensates by opening the throttle further. This was observed during testing. The engine rpm when the vehicle was at idle rose from approximately 600 RPM with no resistance on the supply line to approximately 1000 RPM with a 20 Ω resistance in series with the VCTA signal. A DTC (P0121) was triggered as this resistance value was increased

beyond approximately 20 Ω , resulting in the vehicle transitioning to the fail-safe mode.

- Even though a minimal rise in engine RPM (400 RPM) resulted from the introduced fault condition, the fail-safes in the system operated to prevent a greater rise in engine rpm and wider opening of the throttle valve angle.

5.5.5 Power Supply Variations

Both potentiometers and Hall Effect sensors on throttle circuits require 5 V power from the ECM for operation. The ECM 5 V power supply used by the throttle circuits also powers various other components (including the accelerator pedal sensors, the processors, the throttle motor driver IC and various other sensors). Power supply malfunction can potentially lead to one of the following conditions:

- Power supply under-voltage condition
- Power supply over-voltage condition
- Noisy power supply.

5.5.5.1 Power Supply Under-Voltage

The response of the throttle to an under-voltage condition depends on the type of sensor used in the throttle assembly to detect the throttle valve angle. If the under-voltage condition is due to a series resistance in the VCTA line, the response of the vehicle will be as discussed in section 5.5.4.7. If the under-voltage condition is caused by a drop in the power supply voltage from the ECM, the throttle position sensors, the pedal position sensors, the A/D reference voltage circuit, and other engine sensors will also be simultaneously affected. The response of the vehicle to this condition will be discussed in section 6.6.

5.5.5.2 Power Supply Over-Voltage

The +5 Vdc voltage is generated by the power supply IC. In the event of a failure of the control circuitry within the power supply IC, an output over-voltage condition may occur. This voltage may be as high as the vehicle battery voltage in the worst case condition. The following scenarios may occur under an output over-voltage condition:

- A slight increase in the power supply voltage will not change the behavior of the vehicle, since the same power supply is used for the pedal sensors and the throttle position sensors. Since the sensors in the pedal and throttle body are ratiometric, the vehicle behavior will not change substantially.
- The power supply IC may experience failure modes that result in output voltages that exceed its maximum rating. It is expected that such a failure mode would result in permanent damage to the power supply IC, which would be readily detected. No such observations have been made on vehicles alleged to have experienced UA. In the hypothetical event that the power supply fails such that its output exceeds its rated specifications without causing a permanent failure of the IC, the over-voltage condition may cause components on the ECM to behave abnormally. This analysis is discussed in detail in section 6.6.3.4.
- A large increase in the output voltage exceeding the absolute maximum rating of ICs on the ECM can lead to visible permanent thermal damage to the processors, throttle motor driver IC and/or other components on the ECM. For example, as discussed previously, the Main processor uses the +5 Vdc supply. If the +5 Vdc supply exceeds the absolute maximum rating of the processor, a permanent failure of the processor may result which would affect the generation of the ignition pulses for the ignition coils and the PWM pulses to the throttle motor. This will lead to the vehicle's engine shutting down.

5.5.5.3 Power Supply Variations

Several design features in the ECM (and the Hall Effect based throttle position sensors) mitigate noise and/or ripple on the power supply output. Testing performed to characterize vehicle response to power supply noise is detailed in a separate Exponent report.⁷⁰ The testing did not identify any root cause that would explain reported incidents of unintended acceleration.

5.5.6 Valve Sticking/Stuck Throttle Valve Condition

A mechanically stuck throttle can prevent the throttle valve from responding to commands from the ECM. However, several fail-safes in the system are designed to detect this condition and transition the vehicle to the fail-safe mode or cause the vehicle's engine to shut down. These fail-safes include:

- Throttle valve stuck condition (DTC P2111/P2112)
- Motor over-current condition (DTC P2103)
- System guards (DTC P2119/P1129)

Testing was performed to create a mechanical fault in the throttle body by jamming the throttle plate so that it could not fully close. This was done by using a metal object inserted into the throttle body to obstruct its movement as shown in Figure 79.

⁷⁰ Exponent report: "Evaluation of the Effects of Electromagnetic Fields on the Behavior of Electronic Throttle Control Technology Used in Toyota Vehicles".



Figure 79. Throttle plate stuck partially open by inserting a metal object under the throttle plate.

The testing was performed both on stationary and moving vehicles. Every attempt to jam open the throttle plate was detected by the ECM, resulting in a check engine light, a DTC and the transition of the vehicle to the fail-safe mode.

5.6 Multiple Failures

Testing was conducted to characterize the vehicle response to multiple failures on the throttle circuit. Most multiple failures result in the triggering of a DTC and the transitioning of the vehicle to the fail-safe mode. Failures that did not trigger a DTC resulted in a modest increase in engine rpm during the tests performed. This observed increase could not explain the reported incidents of unintended acceleration.

One specific multiple fault scenario on the throttle circuit involved the introduction of a constant and identical negative voltage offset on both VTA1 and VTA2. This hypothetical multiple fault scenario is similar to the introduction of a series resistive fault in the VCTA line (section 5.5.4.7). Testing indicated that even though a minimal rise in engine RPM can result due to this fault, the fail-safes will operate to prevent a high rise in engine rpm and a large opening of the throttle valve.

Most of the hypothesized multiple fault scenarios require the throttle circuitry to be artificially faulted in a complex and specific fault sequence, using specific resistance values. Most of the hypothesized “faults” result in a detected problem (e.g. triggering a DTC and a fail-safe mode of operation) and/or leave unmistakable physical evidence that would not disappear when the ignition key was cycled. Exponent’s inspections of used vehicle parts, vehicles reported to have experienced unintended acceleration, warranty database reviews, and testing (of vehicles and individual components) have found no evidence that multiple failures occur in the field, or that such failures cause uncommanded acceleration.

5.7 Summary

Exponent’s analysis of the throttle circuit and the testing performed indicated the following:

- The two types of throttle circuit designs used on Toyota vehicles equipped with ETCS-i each contain two throttle valve position detection sensors.
- Failures on the throttle circuitry due to single point resistive faults, power supply variations etc. or hardware failures, cannot explain the reported incidents of unintended acceleration. Typically faults introduced into the throttle circuitry either have no effect on vehicle behavior or trigger a DTC. The worst case vehicle response during testing was a modest increase in the engine RPM at idle. This modest increase cannot reasonably explain the reported incidents of unintended acceleration.
- Should one or more resistive fault develop in the throttle positioning circuitry, such a fault would undoubtedly leave physical evidence on the wiring or on other components of the vehicle (e.g., stains, breached insulation, contamination between wires etc.) that would remain and be detectable after the incident.

6 ECM Hardware

This chapter will discuss the design characteristics of ECMs used on Toyota vehicles equipped with ETCS-i. This will include:

- The purpose of the ECM and its functionality.
- Variations in ECM designs and architecture.
- Variations in the location of the ECMs and design changes.
- ECM construction.
- Major components/subsystems of ECMs involved with throttle control. This will include a description of the functionality of the components/subsystems and also the system response to potential faults. The following ECM subsystems/components will be addressed in this chapter:
 - Filters and protection components
 - Power supply
 - Processors
 - Analog to digital (A/D) converter
 - Throttle motor driver IC.

The testing detailed in this chapter is not intended to provide an exhaustive list of all tests performed on the ECM. None of the testing resulted in an engine response that could reasonably explain the reported incidents of unintended acceleration.

6.1 Introduction

The purpose of the ECM is to control the engine; it acts as the ‘brain’ of the engine. The ECM includes various components and sub-systems. Figure 80 presents a high level block diagram of the ECM showing the main components involved with throttle control.

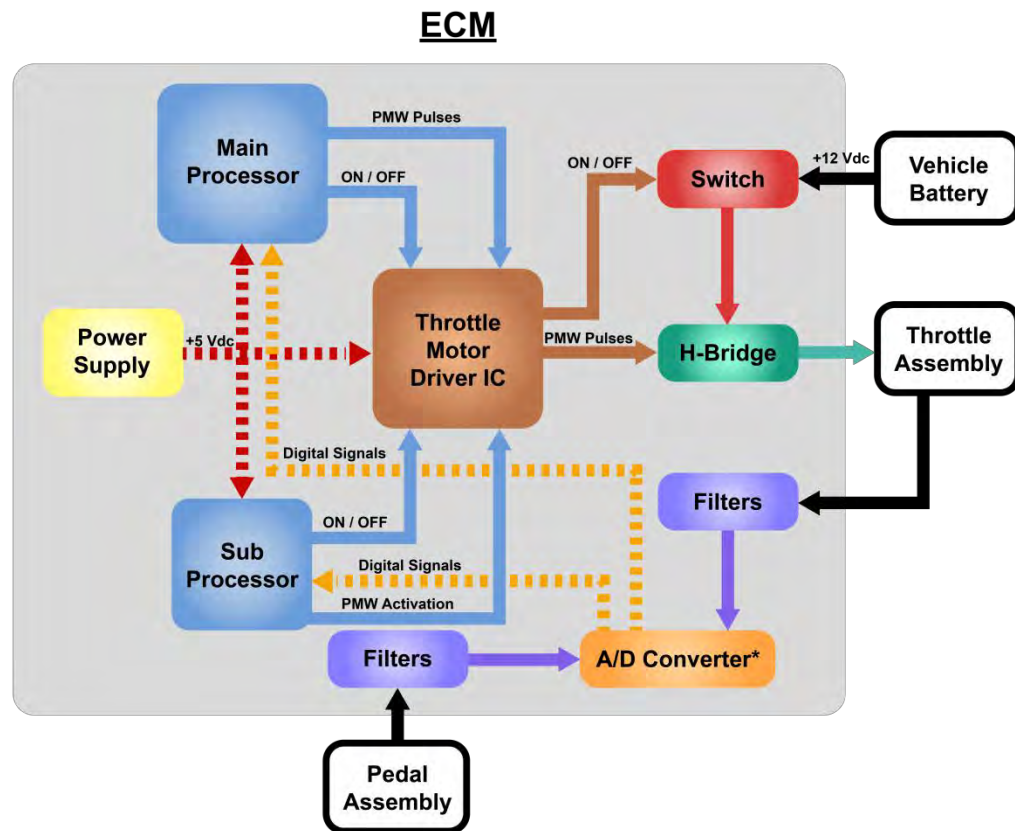


Figure 80. High level ECM configuration for control of the throttle assembly (*In some vehicles the A/D converter is physically located on the same ASIC as one of the Processors).

The following are involved with throttle control:

1. **Signal Filtering Circuits**—A variety of passive pi-filter networks and pull-up/pull-down resistor networks filter noise on the sensor signals
2. **Power Supply**—The power supply IC steps down the vehicle battery voltage, generating the required supply voltages to power the ICs, sensors and other circuits. For example, on a 2007 V6 Camry, a total of 5 power

supply signals (three +5 Vdc and two +1.5 Vdc signals) are generated using a single power supply IC.

3. **Main Processor**—This processor is responsible for calculating the desired throttle valve angle and sending control signals to the throttle motor driver IC. The Main processor can shut off power to the throttle motor if a Class 2 fault is detected (section 3.4). Depending on the vehicle model and engine type, the Main processor may also control additional engine functions, such as fuel injection. In addition to the driver request through the accelerator pedal and/or the cruise control system, a number of sensors in the vehicle provide signals that are used by this processor to calculate the throttle angle. In addition, this processor also monitors the state of the Sub processor and other sub-systems and transitions the vehicle to the fail-safe mode on detecting a failure of one or more of these sub-systems.
4. **Sub Processor**—This processor monitors the operation of the Main processor and other critical subsystems which can affect the throttle valve angle. The Sub processor can transition the vehicle to the fail-safe mode upon detecting a failure of one or more of these subsystems (e.g. the throttle motor driver system etc.). For example, the Sub processor can shut off power to the throttle motor if a Class 2 fault is detected (section 3.4). Depending on the vehicle model and engine type, the Sub processor may also control additional engine functions.
5. **Throttle Motor Driver**—The throttle motor driver IC works in conjunction with an H-bridge to process the pulse width modulated (PWM) signals from the Main processor and drive the throttle motor to move the throttle valve to the desired position. In addition, in some vehicles, the throttle motor driver IC also processes ignition pulses to the spark plug (in the 2007 V6 Camry, the throttle motor driver IC processes four of the six ignition pulses).

The remainder of this chapter will discuss each of the above systems in detail and describe the response of vehicles to a failure of one or more of these systems. The 2007 V6 Camry will be

used for illustrative purposes in this discussion, though differences exist among the various ECMs used in ETCS-i equipped models. Test data from more than one vehicle model may also be presented. The next section will highlight some of the ECM related variations for different Toyota vehicle models.

6.2 ECM Variations

ECM designs have undergone several changes since the introduction of ETCS-i technology in Toyota vehicles. Advancement in technology resulting in improved processing speeds and computational power, advancement in sensing technology and changes in the location of the ECM in the vehicle have all resulted in changes to the ECM hardware.

6.2.1 Number of Processors

As discussed in the introduction, two processors (Main processor and the Sub processor) work together to provide the ECM with its functionality. Some earlier ECM designs contained three processors on the ECM to perform the required functions. The primary functions of the throttle control are contained in the Main processor, and the functions of throttle control system monitoring are contained in the Sub processor. Figure 81 shows a high-level ECM system design with the number of processors used in the ECM for Camry vehicles and their functionality since the introduction of ETCS-i, starting with the 2002 model year vehicle.

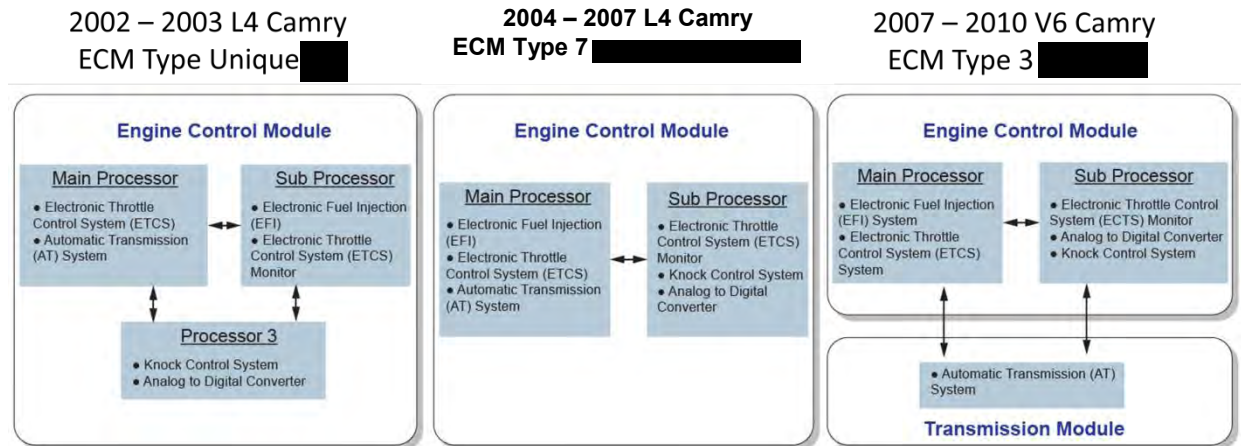


Figure 81. System level hardware configuration for Camry vehicles equipped with ETCS-i.

In addition to the high level system configuration described above, the following other significant changes in hardware design/manufacturing have occurred over the years for Camry vehicles (changes of various types were also made to ECMs of other vehicles at different times).

- Manufacturing of ECMs for Camrys transitioned to the use of lead-free solder during the 2008 and 2009 model years. This coincided with the introduction of nickel-palladium-gold coating for most ICs on the ECM.
- Conformal coating was used on ECMs for 2002 to 2006 model year Camry vehicles (both the L4 and V6 engine variants).
- The ECM was moved from the passenger compartment to the engine compartment starting with the 2007 model year Camry (both the L4 and V6 engine variants). This coincided with the introduction of water-proof connectors for the ECM and a sealed (waterproof) enclosure.

6.3 ECM Construction and Testing

The following will be addressed:

- Housing construction
- Soldering materials
- Operating and storage temperatures
- ECM tests
- Connectors

6.3.1 Housing Construction

The construction of the ECM is dependent upon the location of the ECM in the vehicle. ECMs installed in the passenger compartment (no expected water immersion) have utilized non-waterproof housings, while ECMs located in the engine compartment have utilized water-proof housings.

6.3.1.1 ECMs with Waterproof Housing

ECMs located in the engine compartment use a waterproof housing with waterproof connectors. Figure 82 shows an example of the construction of one such ECM.



Figure 82. ECM from 2007 V6 Camry with waterproof housing.

The construction of the ECM connectors is detailed in Chapter 10.

6.3.1.2 ECMs with Non-waterproof Housing

ECMs located in the passenger compartment (adjacent to the glove box and behind the interior trim panel) are not expected to be exposed to water; the ECM housing fully encloses the electronics and provides protection against contaminant intrusion. Figure 83 shows an example of a non-waterproof ECM from the 2002 V6 Camry.

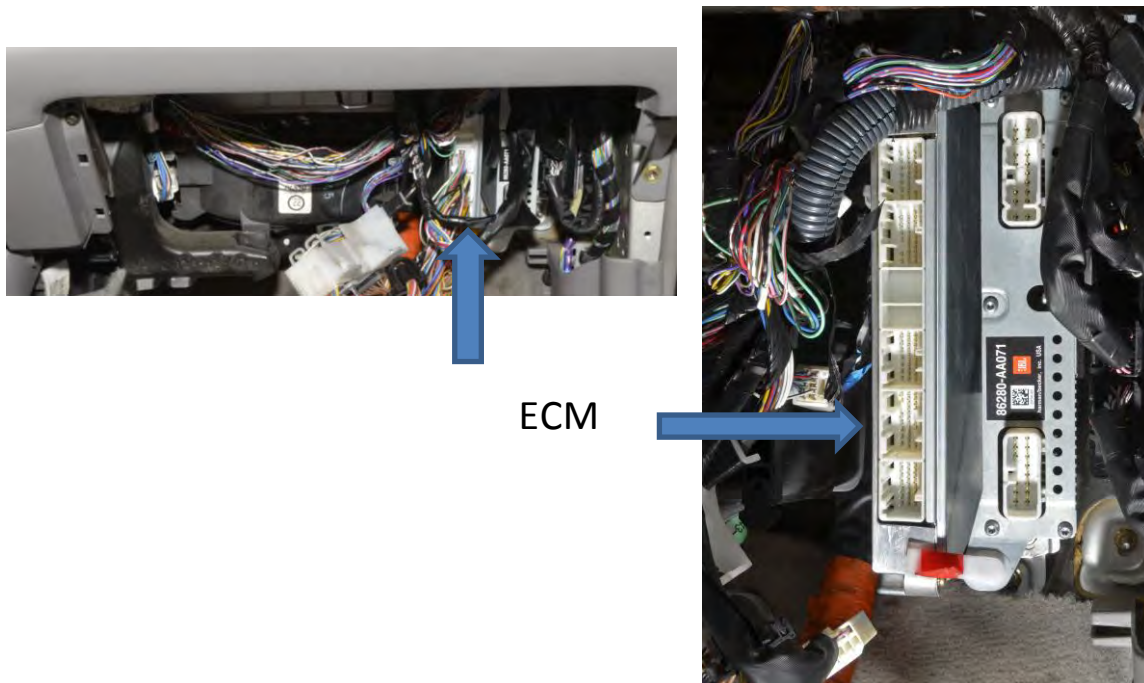


Figure 83. ECM for a 2002 V6 Camry as installed behind the glove box (left). ECM with connectors removed (right).

In addition, conformal coating material is used to provide protection for the electronics against moisture and contamination intrusion in vehicles with ECMs in the passenger compartment. As an example, Figure 84 identifies the conformal coating material on a 2002 Camry, a 2003 Camry and a 2006 Solara ECM.

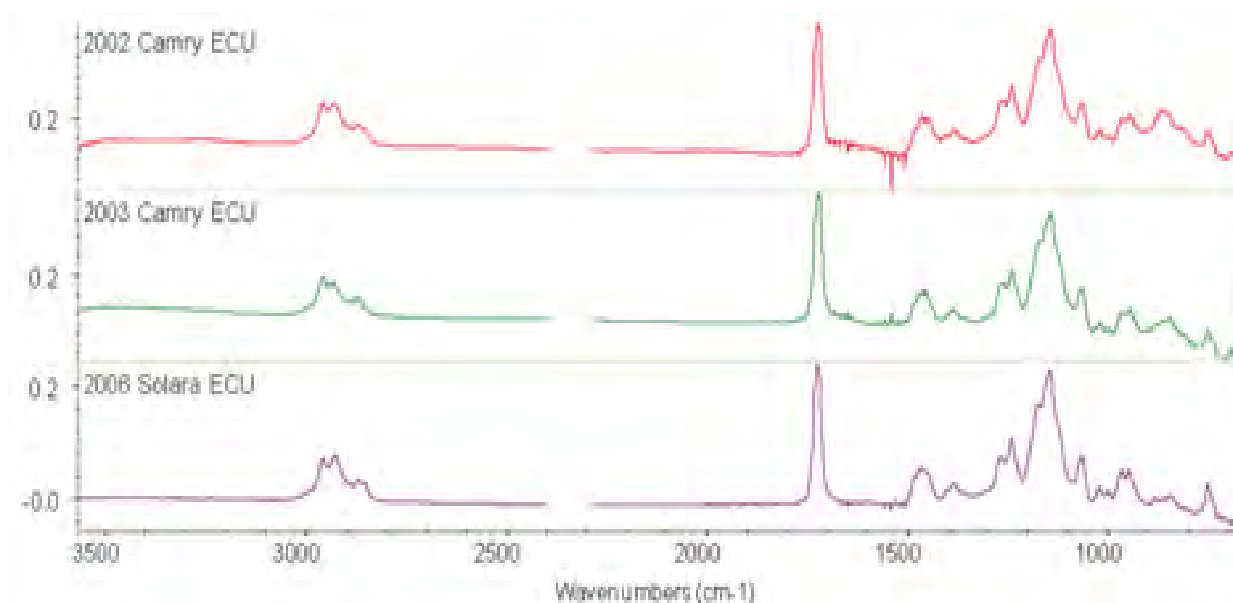


Figure 84. Conformal coating on some ECMs. The FTIR analysis indicates that the coating is a straight acrylic polymer.

6.3.2 ECM Operating and Storage Temperatures

Non-waterproof ECMs located in the passenger compartment are rated for operation from $\blacksquare^{\circ}\text{C}$ to $\blacksquare^{\circ}\text{C}$ and for storage from $\blacksquare^{\circ}\text{C}$ to $\blacksquare^{\circ}\text{C}$. The temperature rating for waterproof ECMs located in the engine compartment is wider. These are rated for $\blacksquare^{\circ}\text{C}$ to $\blacksquare^{\circ}\text{C}$ for operation, and from $\blacksquare^{\circ}\text{C}$ to $\blacksquare^{\circ}\text{C}$ for storage. Exponent's review of the temperature-related test data for Toyota ECMs indicates that the components on the ECM operate within their rated temperature under all conditions.

6.3.3 ECM Tests

Toyota ECMs are subjected to a number of environmental and thermal abuse tests specified in various Toyota Engineering Standards. These tests performed on the ECM (both in the lab and in the vehicles) are designed to validate that sufficient temperature de-rating is provided for all components, and also to validate that all components are rated to handle realistic worst case operating temperature conditions. Tests performed on the ECM include but are not limited to the following:

- Operation test
 - High/low/cycling temperature operation test
- Environmental stress test
 - High/low temperature exposure test
 - Thermal shock test
 - Solder joint life test
 - Temperature/humidity cycle test
 - Migration test
 - Condensation test
 - Drizzle test
- Mechanical Strength Test
 - Vibration test
 - Drop impact test
- Marginal operating temperatures test
 - High/low temperature marginal test
- Electrical noise test
 - Overvoltage test
 - Inverted voltage test
 - Power voltage fluctuation test
 - Ignition pulse test
 - Load dump test

- Field decay test
- Electrostatic discharge test
- Induction noise resistance test
- Radio noise test
- Electromagnetic susceptibility test
- Electromagnetic radiation test
- Narrow-band emission noise test
- Communications test
 - Body multiplex communication test

6.3.4 ECM Connectors

Connectors provide a link between the ECM and the rest of the vehicle, allowing the ECM to receive inputs and to send signals to other systems such as the throttle motor and the spark plugs. The subject of connector design and protection features in connectors used by Toyota is discussed in detail in Chapter 10.

6.4 ECM Design and Theory of Operation

The ECM performs a number of functions, including supplying dc power to sensors, processing signals received from sensors, generating PWM pulses for the throttle motor, monitoring the health of the engine, and activating fail-safes and transitioning the vehicle to a fail-safe mode during a malfunction. The remainder of this chapter will discuss each of the ECM components and the response of the vehicle to faults in these components.

6.5 Filters and Protection Components

At the input to the ECM, the throttle position and accelerator pedal position signals are filtered using individual passive pi-filter networks.⁷¹ In addition, each throttle position sensor signal has a pull-up resistor on the ECM, while each accelerator pedal sensor signal has a pull-down resistor.⁷² In addition, several dedicated components throughout the ECM protect the system and its components against external noise and EMI sources.

6.5.1 EMI/ESD Protection

A wide spectrum of dedicated protection components and circuits are used to improve immunity from electromagnetic interference (EMI) and electrostatic discharge (ESD).

6.5.1.1 EMI

The ECM has multiple layers of protection against EMI. These include the following:

- Dedicated power and ground planes on the multi-layer ECM circuit board
 - Vias⁷³ are used to interconnect the ground plane to corresponding ground locations on other circuit board layers
- Power supply decoupling through low, medium and high frequency decoupling capacitors
- Filtering using passive pi-filters on the ECM

⁷¹ The Hall Effect based throttle position and accelerator pedal position sensors also have filter capacitors at their outputs in the throttle and pedal circuits.

⁷² The pull-up resistors on the throttle position sensor signals would pull the sensor output voltage high if that sensor wire were to open, causing the ECM to detect a near or wide-open throttle condition. The result would be an attempt by the ECM to close the throttle if the driver demand was not for wide open throttle. A DTC would be set almost immediately if VTA1 were pulled high, or when the pedal position was below near-full-throttle request if VTA2 was pulled high. The pull-down resistors on the accelerator pedal position would result in a below-idle voltage signal if that sensor wire were to open, also setting a DTC.

⁷³ A plated-through hole used to connect two or more conductor layers of a multilayer board, in which there is no intention to insert a component lead or other reinforcing material (http://www.ami.ac.uk/courses/topics/0100_gls/glossary/glossv.htm)

- Isolation of the ECM from high voltage ignition coils
- Power supply decoupling on the accelerator pedal circuits and on the throttle position sensor circuits
- Shielded cable for throttle motor power conductors
- Signal cables parallel to ground cable(s) in pedal sensor harness and throttle position sensor harness for cancellation of common mode noise
- Protection components such as capacitors, resistors, diodes (including Zener diodes), and inductors at the input and output terminals
- Anti-parallel diodes in the H-bridge MOSFETs and throttle motor driver IC
- Clamping diodes to protect power supply input from negative transients
- Ground connection to the ECM
- Shielding by grounded vehicle metal housing,

Multiple EMI tests (bulk current injection, chatterbox, anechoic chamber etc.) were conducted by Exponent to assess the effectiveness of the installed protection elements against EMI. The ECM was found to be effectively protected against EMI. Details of this EMI testing are provided in a separate report.

6.5.1.2 Electrostatic Discharge (ESD) and Transient Protection

Multiple levels of ESD and transient protection (both inductive and rapid rise in voltage (dV/dt)) are provided on the ECM for all input and output circuits/pins. For example, on the 2007 V6 Toyota Camry, the following dedicated components/circuits provide protection against ESD:

- Medium and high frequency decoupling capacitors and diodes
- Shielded cables

- Anti-parallel diodes in the MOSFETs and throttle motor driver IC
- Ground plane on the ECM circuit board
- Grounded ECM base plate.

6.5.2 Summary

A review of the circuit design indicates the presence of dedicated components and systems used to provide protection against noise and EMI. Testing performed (detailed in a separate report) found that these components provide adequate protection and prevent external noise from leading to UA. Exponent could not identify any realistic scenarios where external noise and/or EMI could reasonably explain the reported incidents of unintended acceleration.

6.6 Power Supply

The power supply IC converts the vehicle's battery voltage to various voltage levels necessary for powering the on-board circuits as well as sensors in the vehicle. This section will discuss the design of the power supply circuit, the protection features incorporated into the power supply circuit design, and the response of the vehicle to failures of the power supply circuit.

6.6.1 Configuration

A single power supply IC generates several dc voltages that power both the ECM and sensors used by the ECM. A main +5 Vdc power supply voltage is used to power the processors, the throttle motor driver IC, the pedal and throttle electronics and various other sensors. Additional power supply voltages provide power to the processor memory, the relay drivers etc. Table 7 lists the power supply voltages used by selected Toyota vehicles.

Table 7. Power supply voltages used on selected Toyota vehicles⁷⁴

Engine Type	Model Year	Power Supply			
		+ 5 Vdc	+ 3.3 Vdc	+2.5 Vdc	+ 1.5 Vdc
Camry L4	2002–2003	x2 (,)	x2 (,)	N/A	N/A
	2004–2006	x3 (, ,)	N/A	x2 (,)	N/A
	2007–2010	x3 (, ,)	N/A	N/A	x2 (,)
Camry V6	2002–2006	x2 (,)	x2 (,)	N/A	N/A
	2007–2010	x3 (, ,)	N/A	N/A	x2 (,)
LS V8	2002–2003	x2 (,)	x2 (,)	N/A	N/A
	2004–2006	x3 (, ,)	N/A	x2 (,)	N/A
	2007–2010	x3 (, ,)	N/A	N/A	x2 (,)
Tundra V8/UZ	2002	x2 (,)	x2 (,)	N/A	N/A
	2003–2004	x2 (,)	x2 (,)	N/A	N/A
	2005–2006	x3 (, ,)	N/A	x2 (,)	N/A
	2007–2009	x3 (, ,)	N/A	N/A	x2 (,)
Tundra V8/UR	2010	x3 (, ,)	N/A	N/A	x2 (,)

As an example, on the 2007 V6 Camry, the power supply IC is used to generate five independent, regulated outputs. The five supply outputs on the 2007 V6 Camry are:

1. +5.0 Vdc powers major components involved with throttle control. These include the Main processor, the Sub processor, the throttle motor driver IC, the analog to digital converter, I/O devices, the two accelerator pedal sensors, the two throttle position sensors etc.

⁷⁴ Vc refers to the main +5 Vdc power supply voltage.

2. +5.0 Vdc for the Main relay driver on the Sub processor.
3. +5.0 Vdc for the CAN bus logic.
4. +1.5 Vdc for the Main processor SRAM.
5. +1.5 Vdc for the Main processor core.

The remainder of this section will discuss the protection features and system response to failures of the power supply IC.

6.6.2 Filtering

Transient protection at the input, and filtering at the input and output of the power supply IC are employed to minimize variations in the power supply output voltages and to mitigate interference that has the potential to affect operation of components and systems that use the power supply output. Various decoupling capacitors are used to filter the power supply output. As an example, low, medium and high frequency decoupling capacitors on the dc buses filter the power supply output on the ECM of a 2007 V6 Camry. Additional noise immunity is achieved through the use of dedicated power and ground planes on the ECM circuit board. An analysis of the filtering components and circuits used indicates that the selection of the capacitors limits variations in power supply outputs due to noise.

6.6.3 Potential Failure Modes

This section discusses the potential failure modes of the power supply IC and the system response to these failure modes. A 2007 V6 Camry will be used as an example to describe vehicle response to the failure modes. Representative test results will be detailed in this section. The intention of this section is not to include all the tests performed on the power supply, but to relate testing to the failure mode investigation. The following failure modes will be discussed in this section:

- Output overload
- Output short-circuit
- Under-voltage
- Over-voltage
- Over-temperature
- Electrical noise and voltage transients
- Latch-up.

6.6.3.1 Output Overload

An output overload of one or more power supply output signals can lead to a loss of the output voltage. The power supply IC includes an internal over-current protection circuit that shuts down the power supply and prevents an over-current condition from causing permanent failure. The output currents from all the power supply circuits are monitored by the power supply IC. This information is used to limit the output current to the loads connected at the output of the power supply IC.

If a fault results in an overload condition where the current exceeds the power supply reserve capacity⁷⁵, the power supply design causes a drop in the power supply output. As an example, Figure 85 shows the V-I characteristics of the main +5 Vdc power supply for a 2005 V6 Camry. The output voltage of the power supply starts to drop due to the overload condition. During testing performed on a vehicle, it was observed that the vehicle's engine shut down when this voltage dropped to approximately 3.5 V.

⁷⁵ As an example, on the 2007 V6 Camry, the main power supply output (+5 Vdc) has a reserve capacity of approximately 100%. Hence, in the event of an overload condition, the power supply IC is capable of supplying a load current which is approximately double the normal load current.

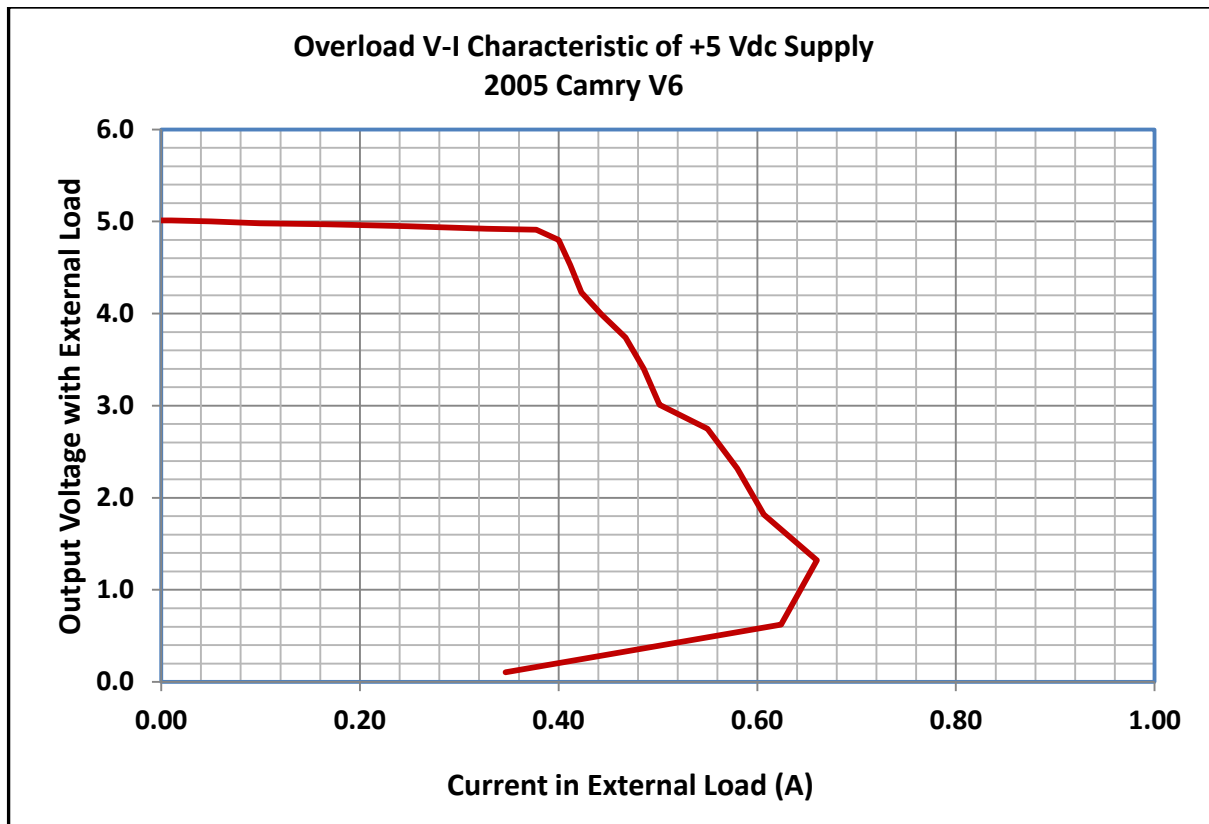


Figure 85. Overload V-I Characteristic of the main +5 Vdc Supply for a 2005 Camry V6.

The system design ensures that if an overload condition occurs, a drop in the power supply output voltage will result in the engine shutting down, preventing an overload on the +5 V supply from causing UA.

6.6.3.2 Power Supply Short-Circuit

A short circuit at the output of the power supply leads to a drop in the output voltage. If the output voltage of the main power supply drops below approximately 3.5 V, the vehicle's engine shuts down (section 6.6.3.1). Testing conducted on a 2007 L4 Camry demonstrated an immediate shut down of the vehicle's engine on the application of a short circuit at the output of the power supply.

6.6.3.3 Under-Voltage

A low voltage output may result due to an output overload condition (section 6.6.3.1), or a failure of the power supply IC. Testing performed on a 2009 V6 Camry to simulate an output under-voltage indicated that the vehicle continued to work as normal until the power supply output voltage dropped to approximately 3.5 V, at which point the vehicle's engine shut down. In addition, because the Hall Effect sensors in both the accelerator pedal and the throttle assembly are powered by the main +5 Vdc power supply and are ratiometric, no increase in vehicle rpm occurs (either when the vehicle is at idle or being driven) as the power supply voltage drops from +5 V to + 3.5 V.

6.6.3.4 Power Supply Over-Voltage

An output over-voltage condition may occur in the event of a failure of the control circuitry within the power supply IC. The output voltage may be as high as the vehicle battery voltage in the worst case condition. The following faults may occur:

- A slight increase in the output voltage will not change the behavior of the vehicle if this voltage does not exceed the maximum voltage rating of the processors and other components on the ECM
- A large increase in the output voltage that exceeds the absolute maximum rating of the ICs can lead to permanent damage to the processors, throttle motor driver IC and/or other components on the ECM. For example if the +5 Vdc supply exceeds the absolute maximum rating of the processor⁷⁶, a permanent failure of the processor may result. This will prevent the generation of the ignition pulses for the ignition coils and the PWM pulses to the throttle motor, which will cause the vehicle's engine to shut down. In addition, such a failure would be permanent and visible after the incident. Permanent failures of the ECM cannot reasonably explain the reported incidents of unintended acceleration.

⁷⁶ As an example, the Main processors and Sub processor on the ECM of a 2007 V6 Camry are rated for an absolute maximum voltage of 6 Vdc.

- Failures where electronic components on the ECM exhibit abnormal behavior (as opposed to a complete shut-down) were also considered. In this scenario, the power supply IC was hypothesized to have failed such that the output voltage was higher than the absolute maximum rating of one or more components on the ECM, but not high enough to lead to a destructive failure of the component(s). This condition may cause the components to function abnormally. The vehicle response in this condition will depend on the component that starts to function abnormally. Table 8 provides details of possible vehicle response under this condition.

Table 8. Vehicle response to abnormal operation of components on the ECM due to an over-voltage condition

Component	Vehicle Response
Main Processor	Section 6.7.3 details vehicle response to abnormal operation of the Main processor.
Sub Processor	Section 6.7.3 details vehicle response to abnormal operation of the Sub processor.
Throttle Motor Driver IC	Section 6.9.3 details vehicle response to abnormal operation of the throttle motor driver IC
Sensors in Throttle /Pedal Assembly	The sensors in the throttle assembly and the pedal assembly are rated for an absolute maximum voltage that exceeds █ V. Other sub-system failures will occur at voltages lower than those necessary to cause abnormal operation of the Hall Effect sensors.
A/D Converter	Section 6.8.1.1 details vehicle response to abnormal operation of the A/D converter.

A failure of the power supply IC resulting in an overvoltage condition would likely be permanent and observable even when the ignition is turned off and on. If the failure is not destructive and affects the operation of one or more components on the ECM, several safeguards will prevent the condition from leading to UA. No mechanism has been found where a power supply over-voltage condition would result in UA.

6.6.3.5 Electrical Noise and Voltage Transients

Section 6.5 details the protection components and circuits utilized to filter the power supply output(s). Multiple EMI tests verified that the installed protection elements provide adequate electrical noise protection. Details of this EMI testing are provided in a separate report.

6.6.3.6 Over-Temperature

The power supply IC is manufactured using silicon-on-insulator (SOI) technology which enhances the high temperature and high voltage performance of the IC. Each IC package is also manufactured to reduce operating temperatures. Test data reviewed by Exponent indicates that the power supply IC is designed with adequate temperature derating. Although the analysis and document review performed by Exponent does not give any indication of the power supply IC failing due to an over-temperature condition, temperatures outside the rating of the power supply IC may cause the power supply IC to function incorrectly and output a voltage that deviates from its rated output. As discussed in sections 6.6.3.3 and 6.6.3.4, this condition will not lead to UA.

6.6.3.7 Latch-up

The power supply IC is manufactured using SOI technology, which is an effective prevention mechanism against latch-up. The power supply IC is also tested in accordance with microelectronics industry standard JEDEC/JESD78: "IC Latch-up Test" to ensure that it is not susceptible to latch-up. Even if a latch-up of the power supply IC were to occur, the IC's internal over-current protection circuit will activate, providing an additional layer of protection. If this layer of protection fails, the over-current condition will likely cause damage to the IC that will remain visible after the incident. In the event that the latch-up condition does not lead to destructive and permanent damage to the IC, it may start to function incorrectly and output a voltage that deviates from its rated output. As discussed in sections 6.6.3.3 and 6.6.3.4, this condition will not lead to UA.

6.6.4 Summary

No failures of the power supply IC were identified that would lead to UA. Testing and analysis performed on the power supply IC and related circuitry demonstrates that:

- The filter circuits used on the power supply circuit provides adequate protection against external noise and other EMI sources
- A latch-up condition of the power supply IC, though mitigated through the use of SOI technology, would nevertheless cause the vehicle to shut down and likely lead to permanent damage to the IC
- All other potential failure modes of the power supply circuit would cause no change in vehicle operation, or cause the vehicle's engine to shut down preventing UA.

Exponent could not identify any faults of the power supply IC that could reasonably explain the reported incidents of unintended acceleration.

6.7 Processors

Processors on the ECM are responsible for many functions, including but not limited to processing the information from various sensors, generating ignition coil firing signals, throttle valve adjustments, and fuel-injection control. These processors also monitor the health of the engine and the subsystems and activate fail-safes in the event of malfunctions.

6.7.1 Main Processor

The Main processor is responsible for integrating the driver's request and the signals from sensors and calculating the desired throttle valve angle. Figure 86 is a high level block diagram depicting the processing of signals from the pedal, the cruise control subsystem, the Vehicle

Stability Control (VSC) and Electronically Controlled Transmission (ECT) computer and other systems. The 2007 V6 Camry is taken as an example for the discussion.

- The signals from the two pedal position sensors (VPA1 and VPA2) are digitized by the A/D converter and processed in the Main Processor. The Main processor calibrates the two signals by comparing them with the learned idle position value of the signals (section 4.5).
- After range checking and comparison of the processed values, a non-linear conversion is applied to determine the desired throttle angle. This angle is compared with the throttle request from the cruise control module and the maximum of the two values is selected ('Driver Request' in Figure 86).

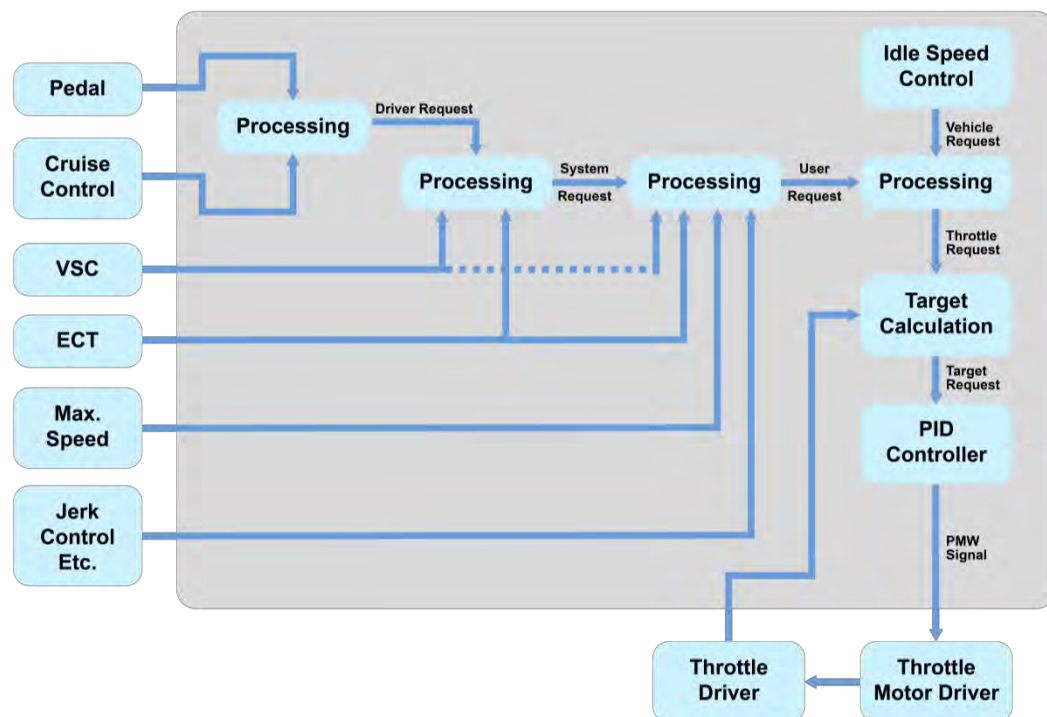


Figure 86. Software architecture for throttle control on the 2007 V6 Camry.

- The 'Driver Request' is processed along with the throttle opening request from the Vehicle Stability Control (VSC) and the Electronically Controlled

Transmission (ECT) computers, to generate the 'System Request' signal (Figure 86).

- Request from ECT computer:
 - The ECT computer does not send a request to the ECM to open the throttle. The ECT computer is only capable of sending a request to close the throttle.
 - The ECT computer communicates with the ECM via the CAN bus. In the event of a failure of the ECT computer, it is expected that its communications with the ECM via the CAN bus will cease.
 - In the event that the ECT computer fails in a manner that it requests a large throttle opening, a DTC (P2119) will be triggered if the throttle opening request exceeds approximately 3° when the vehicle is at idle, or approximately 25° when the vehicle is being driven (section 7.9.2). In the event that the request from the failed ECT computer is less than approximately 25°, the ECM will fulfill the request and open the throttle valve. However, as soon as the vehicle starts to accelerate, the expected driver response will be to release the pedal, which will transition the vehicle to the idle mode (where a DTC is triggered, if the ECT throttle opening request exceeds approximately 3°). This will trigger a DTC (P2119) transitioning the vehicle to the fail-safe mode.
- Request from VSC computer
 - The VSC computer handles the vehicle stability control functionality, the traction control functionality and the anti-lock brake system (ABS) functionality. The design of the VSC computer is different for different model year Camry vehicles.

- The traction and ABS systems are not designed to request a throttle opening under any operating condition
 - The VSC system for 2002 to 2006 model year Camry vehicles is not designed to request a throttle opening under any operating condition. However, the VSC system in 2007 and later model year Camry vehicles, has the ability to request a limited throttle opening in order to reduce the engine braking power.
 - The VSC computer communicates with the ECM via the CAN bus. In the event of a failure of the VSC computer, it is expected that communications with the ECM via the CAN bus will cease.
 - In the event that the VSC computer fails in a manner that it requests a large throttle opening, a DTC (P2119) will be triggered if this request exceeds approximately 3° when the vehicle is at idle or approximately 25° when the vehicle is being driven (section 7.9.2). In the event that the request from the failed VSC computer is less than approximately 25°, the ECM will fulfill the request and open the throttle valve. However, as soon as the vehicle starts to accelerate, the expected driver response will be to release the pedal, which will transition the vehicle to the idle mode (where a DTC is triggered if the VSC throttle opening request exceeds approximately 3°). This will trigger a DTC (P2119) transitioning the vehicle to the fail-safe mode.
- A number of bound checks through the minimum block are performed on the ‘System Request’ signal (generating the ‘User Request’ signal in Figure 86) to ensure that the vehicle does not increase its maximum speed setting and

does not have large step changes in the throttle opening request signal (for example to prevent the vehicle from sudden jerks etc.).

- A variety of electrical loads in the vehicle (e.g. air conditioner) also provide input into the amount of throttle valve opening. Requests from these electrical loads are processed by the Idle Speed Control (ISC) system.
 - A bounds check is performed on the request from all the electrical loads in the vehicle to ensure that the throttle opening request from the ISC system ('Vehicle Request' in Figure 86) does not exceed 15.5°.
- The 'Vehicle Request' signal is summed with the 'User Request' signal to generate the 'Throttle Request' signal, which is the desired throttle opening angle based on the input from the driver, cruise control and the vehicle's electrical loads.
- Feedback from sensors in the throttle assembly is combined with the 'Throttle Request' signal to generate the final 'Target Request' signal
- The 'Target Request' signal is processed by a proportional-integral-derivative (PID) control system to generate pulse width modulated (PWM) signals which are then used by the throttle motor driver circuit to move the throttle valve.

The description above gives the general operation of how the throttle angle is calculated and also describes how the commanded angle is constrained to follow the driver request without allowing significant deviations that may lead to wide open throttle. The operation of the system in this manner inherently acts as one of the many protection layers in the software against UA.

In addition to calculating the desired throttle valve opening angle, the Main processor also performs various diagnostic functions. Checks in the Main processor are designed to monitor input signals from sensors and to transition the vehicle to a fail-safe mode upon detecting a failure. Checks performed by the Main processor include the following:

- State of health of the throttle motor to detect a locked motor, a short-circuited motor, etc.
- State of health of the throttle position sensor signals to detect a deviation in the outputs from their expected values, a short circuit between the outputs, an open-circuit failure, etc.
- State of health of the pedal position sensor signals to detect a deviation in the outputs from their expected values, a short circuit between the outputs, an open-circuit failure of the sensors, etc.
- Monitoring the operation of the Sub processor through a watchdog.

6.7.2 Sub Processor

The Sub processor is contained in an ASIC that performs several functions. In addition to the Sub processor, the ASIC contains other modules that include:

- Analog-to-digital (A/D) converter
- Direct memory access (DMA).

A global bus is used for communication between the various modules on the ASIC. The Sub processor is a diagnostic processor which monitors the state of the Main processor and various other input and output signals. The Sub processor monitors the following:

- Operation of the Main processor
- The overall system; detects a system level failure of the calculation algorithm in the Main processor and/or hardware on the ECM which causes a deviation in the throttle position from its expected position.
- The throttle motor driver algorithm and hardware circuit

- State of health of the throttle position sensor signals to detect a deviation in the outputs from their expected values, a short circuit between the outputs, an open-circuit failure, etc.
- State of health of the pedal position sensor signals to detect a deviation in the outputs from their expected values, a short circuit between the outputs, an open-circuit failure of the sensors, etc.
- Serial communication block

6.7.3 Failure Modes

This section details hardware-related failure modes of the two processors and the vehicle's response to a failure of the processors. A failure of these processors could occur due to many reasons including external stresses (electrical, environmental etc.), chip failure, contamination leading to pin-to-pin shorts, etc. The following failure modes will be discussed in this section:

- Processor failure
- Under-voltage
- Over-voltage
- Over-temperature
- Electrical noise and transients
- Latch-up
- Pin-pin faults
- Bit flips/memory errors

6.7.3.1 Abnormal Operation

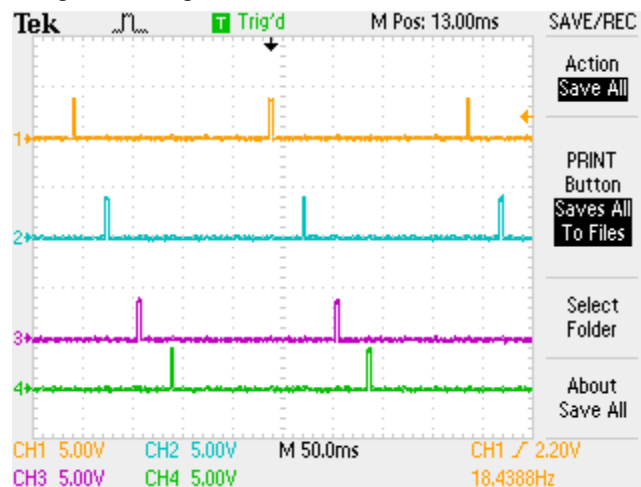
A number of failure modes can lead to abnormal operation of the processors. Exponent has performed a detailed analysis of various abnormalities that may be exhibited by the processors

and the corresponding vehicle response to these abnormalities. Table 9 provides an overview of the highlights of this analysis. Subsequent sections that discuss the various failure modes of the Main processor or Sub processor will use Table 9 as a reference.

Table 9. Vehicle response to abnormal operation of the processors on the ECM

Component	Vehicle Response
Main Processor	If the portion responsible for communications with the Sub processor operates abnormally, inconsistent communication between the Main Processor and the Sub Processor will result, leading to a communication fault which will trigger DTC P0606 and transition the vehicle to the fail-safe mode.
	If the portion of the processor that generates the trigger pulses for the ignition coils starts to operate abnormally, the vehicle will shut down ⁷⁷ .
	If the portion of the Main processor that generates the watchdog service pulse to the power supply starts to operate abnormally, the frequency of these pulses will change resulting in the power supply resetting the processor and causing the vehicle's engine to shut down
	If the algorithm that calculates the desired throttle opening request from the pedal request to malfunction, a condition may arise where the throttle opening request from the processor exceeds the pedal request.

⁷⁷ Each ignition coil in the vehicle receives a trigger pulse from the ECM. The Main processor generates the trigger pulses in the proper sequence. For example, the figure below shows the ignition pulses generated for four of the six ignition coils on a 2009 V6 Camry. The ignition coils require the generation of these pulses in a proper sequence to allow the engine to operate. Abnormal operation of the portion of the processor responsible for the generation of these pulses will result in either a timing issue with the generation of the ignition pulses or a complete termination of the ignition pulses, both of which will lead to the vehicle's engine shutting down.



Ignition pulses for four of the six ignition coils on a 2009 V6 Camry

Component	Vehicle Response
	<p>In this condition, a DTC (P2119) will be triggered (by the Sub processor) if the throttle opening request from the Main processor exceeds the non-linearly corrected pedal request by approximately 3° when the vehicle is at idle or approximately 25° when the vehicle is being driven (section 7.9.2).</p> <p>In the event that the throttle opening request exceeds the non-linearly corrected pedal request by more than 3° but less than approximately 25°, the throttle valve will be opened to the incorrectly calculated angle. However, as soon as the vehicle starts to accelerate, the expected driver response will be to release the pedal, transitioning the vehicle to the idle mode where a DTC is triggered, if the throttle opening request exceeds the non-linearly corrected pedal request by approximately 3°.</p> <p>Abnormal operation of the Main processor may also affect other systems controlled by the Main processor e.g. spark timing, fuel injection etc. These sub systems can at worst cause a minor speed increase (which is easily controlled by an application of the brake or releasing the pedal). Minor speed increases due to abnormal operation of the Main processor that affects these systems is not consistent with the reported incidents of unintended acceleration.</p>
Sub Processor	<p>The throttle opening angle calculation and the generation of the PWM pulses to drive the throttle motor is performed by the Main processor. Hence, abnormal operation of the Sub processor cannot lead to UA⁷⁸.</p> <p>Abnormal operation of the Sub Processor can also lead to inconsistent communication with the Main Processor. This will lead to a communication fault and will trigger DTC P0606 which will transition the vehicle to the fail-safe mode.</p>

⁷⁸ The Sub processor has the ability to disrupt power to the throttle motor driver circuit. Disruption of power to the throttle motor driver circuit can cause the throttle valve to transition to an unpowered state causing the valve to revert to an angle of 6° by the springs in the throttle body.

6.7.3.2 Processor Failure

Watchdog timers are used to monitor the operation of the processors. For example, in a 2007 V6 Camry, the power supply IC receives periodic signals from the Main processor and resets the processor if those signals stop. Similarly, the Main processor monitors the state of the Sub Processor, resetting the processor in the event of a failure of this processor. This configuration is depicted in Figure 87. A resetting of the Main and/or the Sub processor turns the vehicle's engine off.

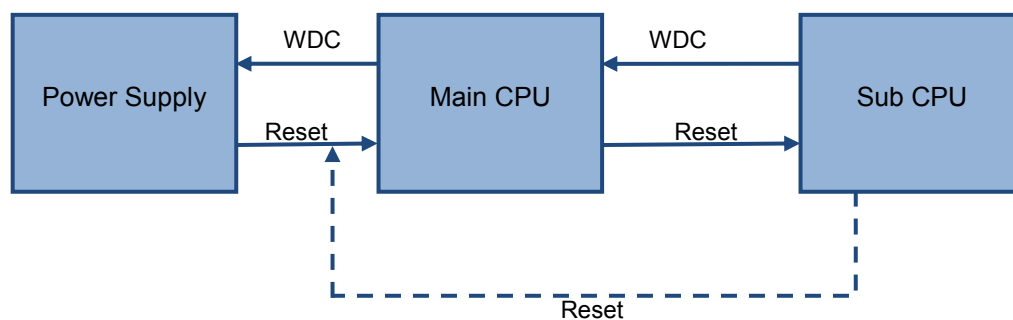


Figure 87. Watchdogs and processor failures (WDC: watchdog counter).

A test was performed to characterize the vehicle response to a failure of one of the processors and to verify the operation of the reset functionality. During this test, a communication failure between the two processors was simulated by individually disconnecting pins on the processors in the ECM of a 2009 V6 Camry. Both the data and signal pins were disconnected during the test. Testing demonstrated that:

- A loss of communication between the two processors immediately results in the vehicle's engine shutting down.
- If no communication occurs between the two processors the vehicle's engine cannot be started.

The testing indicated that a failure of either the Main processor or the Sub processor resulting in the inability of either processor to communicate with the other or to update the watchdog will

cause the vehicle's engine to shut down. Hence, a failure of one or both processors that are involved with throttle control will not lead to UA.

6.7.3.3 Under-Voltage

The processors used in the ECM on Toyota vehicles are rated for operation up to 5 V. The ECM uses a 5 V power supply for the processors. By design, the processors are reset if the power supply voltage drops below a certain threshold. For example on the 2007 V6 Camry, the power supply is designed to reset the processors if the main power supply output drops below approximately 4.5 V. A reset of the processor results in the vehicle's engine shutting off. Testing performed on a 2007 L4 Camry, a 2002 V6 Camry and a 2007 V6 Camry indicated that the ECM continued to operate as normal for power supply voltages down to approximately 3.5 V, with the vehicle shutting down when the power supply voltage dropped below approximately 3.5 V.

6.7.3.4 Over-Voltage

An over-voltage condition may result in the failure of the Main and/or the Sub processor. Such a failure will lead to one of the following conditions:

- Main Processor
 - A failure of the Main processor due to an over-voltage condition will be detected by the Sub processor, which will transition the vehicle to the fail-safe mode. In addition, the failure of the Main processor will cease the generation of the trigger pulses for the ignition coils and prevent the fuel injection process, both of which will cause the vehicle's engine to shut down. The loss of communication with the Sub processor will also cause engine shutdown. The failure of the Main processor may be permanent and observable even when the ignition is turned off and on.

- An over-voltage condition may also cause the Main processor to operate abnormally. The consequences and vehicle response to abnormal operation of the Main processor are discussed in Table 9.
- Sub Processor
 - A failure of the Sub processor due to an over-voltage condition will result in loss of communication with the Main processor, and a loss of updating of the WDC, which will lead to the Sub processor being reset by the Main processor and an engine shutdown. In addition, this failure of the Sub processor may be permanent and observable even when the ignition is turned off and on.

An over-voltage condition may also cause the Sub processor to operate abnormally. The consequences and vehicle response to abnormal operation of the Main processor are discussed in Table 9.

6.7.3.5 Over-Temperature

As discussed in section 6.3.2, the ECM is rated for operation up to ■■■°C for ECMs installed in the passenger compartment and for up to ■■■°C for ECMs installed in the engine compartment. The Main processor IC is rated for operation from ■■■°C to ■■■°C, while the Sub processor IC is rated for operation from ■■■°C to ■■■°C.⁷⁹ Exponent reviewed test data for the operating temperatures of various components on the ECM under various operating conditions. Although the analysis and document review performed by Exponent does not provide any indication of either the Main processor or the Sub processor failing due to an over-temperature condition, temperatures that are outside the rating of the processors may cause them to function abnormally. Abnormal operation of the processors is discussed in Table 9.

⁷⁹ For the 2007 V6 Camry

6.7.3.6 Electrical Noise and Transient Over-Voltage

Electrical noise can affect the operation of the processors, causing communication errors, bit flips etc. Several dedicated design features provide protection against electrical noise. In addition, EMI testing performed by Exponent on the ECM and the entire ETCS-i system did not identified a root cause that would explain the reported incidents of unintended acceleration.

6.7.3.7 Latch-up

A latch-up of either processor cannot realistically occur in the field and lead to UA for a variety of reasons. These include:

- Both processors are tested in accordance with industry standard JEDEC /JESD78: “IC Latch-Up Test” to ensure that the ICs are not susceptible to latch-up.
- An analysis of the system design and testing performed on vehicles indicates that a latch-up of either the Main processor and/or the Sub processor will not lead to UA but will cause the vehicle’s engine to shut down.
- The following will occur if either the Main processor or the Sub processor latch-up:
 - Main Processor:
 - A latch-up of the Main processor or portions of the Main processor can cause the processor to operate abnormally. The consequences and vehicle response to abnormal operation of the Main processor are discussed in Table 9.
 - The latch-up condition can also cause the power supply output voltage to drop to approximately 2 V or less (section 8.3). This will lead to a reset of both processors causing the vehicle’s engine to shut down.

- Sub Processor:
 - A latch-up of the Sub processor or portions of the Sub processor can cause the processor to operate abnormally. The consequences and vehicle response to abnormal operation of the Sub processor are discussed in Table 9.
 - A latch-up condition on the Sub processor can cause the power supply output voltage to drop to approximately 2 V or less (section 8.3). This will lead to a reset of both processors causing the vehicle's engine to shut down.

An analysis of the ECM and system design in addition to testing performed by Exponent indicates that a latch-up of either the Main and/or the Sub processor will not lead to UA but will cause the vehicle to transition to the fail-safe mode or the vehicle's engine to shut down.

6.7.3.8 Pin-Pin Fault

Shorts between adjacent pins on either the Main processor or the Sub processor can lead to a variety of problems, including incorrect inputs to the processors or modifications in the output signals from the processor(s). These shorts can arise from contamination or conductive filaments such as tin whiskers on uncoated boards, solder bridges etc. The following section discusses concerns that might affect pin-to-pin shorts on the processors.

6.7.4 Toyota Tin Whisker Testing

In preparation for the introduction of lead-free electronics in 2008, Toyota implemented tin whisker testing and inspection processes, generally consistent with US, Japanese, and European

Union industry standards,^{80,81,82} Toyota's particular test parameters were developed through evaluation of worst-case environments for whisker growth.

6.7.5 ECM Inspections and Testing

Exponent inspected ECMs from model years 2002 to 2009 according to National Aeronautics and Space Administration (NASA) and industry guidelines, using both optical and scanning electron microscopy. Board solders and solderability platings, as well as component platings were evaluated for composition using energy dispersive spectroscopy. Conformal coatings were analyzed with optical microscopy for thickness and Fourier-transform infrared spectroscopy for composition. Pin-to-pin shorting experiments were also performed on all adjacent pin pairs of the Main processor and Sub processor of the engine control module (ECM) of a 2007 L4 Camry to assess the consequences of shorting.

Camry ECMs utilize varying levels of technologies for prevention or minimization of tin-whisker induced shorting. These include:

- Eutectic tin-lead solders and solderability finishes up to the 2008 model year⁸³
- Nickel-palladium-gold or eutectic tin-lead solder platings on critical integrated circuits (the Main processor, Sub processor, power supply IC, and throttle motor driver IC)

⁸⁰ JEDEC Solid State Technology Association standard JESD201, "Environmental acceptance requirements for tin whisker susceptibility of tin and tin alloy surface finishes," March 2006.

⁸¹ Japanese Electronics and Information Technology Industries Association (JEITA) standard ET-7410, "Whisker test methods on components for use in electrical and electronic equipment," December 2005.

⁸² IEC standard 60068, Edition 1, "Environmental testing – part 2-82: whisker test methods for electronics and electric terminals," 2007.

⁸³ The Main and Sub processors of the Camry ECMs were not tin plated for model year 2002 to 2007 Camry vehicles. Hence, these vehicles are only susceptible to shorting if a tin whisker grows to a sufficient length on an adjacent component, breaks off, and then moves across the board (by vibration, etc.) to the pins. Such shorting can be eliminated as a failure mode owing to the use of conformal coatings in some model years.

- Nickel-underplating between matte tin platings and copper leadframes
- Acrylic conformal coatings (25-40 microns) up to the 2007 model year.

Exponent inspected ECMs from Camry vehicles equipped with ETCS-i systems. No whiskers longer than 40 microns were observed in any of these inspections. (Details of Exponent's analysis are provided in Appendix F.)

6.7.5.1 Pin-to-Pin short and resistance testing

To simulate the effects of a tin whisker, Exponent induced both a short-circuit condition and a low-resistance fault condition (30 Ω) between adjacent pins on both the Main processor and the Sub processor of a 2007 L4 Camry. Approximately 660 test runs were performed (see Appendix E for details). The majority of test runs did not result in any change in engine rpm. Of the 660 tests:

- Sixty (60) tests resulted in the engine shutting down
- Thirty-seven (37) different DTCs were triggered
 - 2500 RPM was the highest RPM observed. This increased engine speed was momentary, lasting a few seconds before a DTC was set.

Testing indicated that a pin-pin fault (short-circuit and/or resistive) will not lead to a wide open throttle condition or cause UA. Pin-to-pin shorting cannot explain the reported incidents of unintended acceleration.

6.7.5.2 Bit Flips/Memory Errors

A memory error or bit flips on registers in either the Main processor or the Sub processor can lead to incorrect operation. Several software features such as software mirroring, diagnostic modules etc. have been implemented to address potential bit flips and memory access concerns.

The analysis and testing of these software features are discussed in detail in Chapter 7. Random bit flips or memory errors were ruled out as potential causes for unintended acceleration.

6.7.6 Summary

This section discussed hardware related failures of the two processors. Exponent's testing and analysis has identified no failures of either the Main processor or the Sub processor that would lead to unintended acceleration.

6.8 Analog to Digital Converter

The A/D converter is located on the Sub processor ASIC.⁸⁴ The A/D converter is a -bit converter that digitizes signals from both the throttle and pedal, in addition to signals from other sensors.⁸⁵ The A/D converter communicates with the serial communication block on the ASIC, which interfaces with the Main processor.

The A/D converter module is composed of a digital control block and an analog control block and includes a multiplexer to selectively switch the sensor signals to the input of the A/D converter. The A/D conversion is performed sequentially using a pre-set priority system.

The converter is powered by the same regulated + 5 Vdc (Vc) power supply that supplies dc power to the Main and Sub processors, the sensors on both the pedal and the throttle body and a number of other sensors (MAF sensor, IAT sensor, oxygen sensor etc.) in the vehicle.

6.8.1 Failure Modes

The following sections will discuss the system response to a failure of the A/D converter. The following failure modes will be discussed in this section:

⁸⁴ On the 2007 V6 Camry ECM

⁸⁵ For example signals from the Mass Air Flow (MAF) sensor, the oxygen sensor, the intake air temperature (IAT) sensor etc.

- A/D converter failure
- Under-voltage
- Over-voltage
- Over-temperature
- Electrical noise and transients
- Latch-up
- Cross-talk
- Drift in reference voltage signal.

6.8.1.1 Abnormal Operation

A complete failure of the A/D converter will result in a loss of communication between the A/D converter and the processors which will prevent the vehicle from functioning. However, Exponent considered the possible consequences of failure modes that may lead to abnormal operation of the A/D converter. An overview of the highlights of this analysis follows.⁸⁶ In subsequent sections that discuss the various failure modes of the A/D converter, the details that follow will serve as a reference for the vehicle response to the failure modes.

The vehicle response to abnormal operation of the A/D converter depends on the condition that causes the abnormal operation. Possible scenarios are:

- If the A/D converter circuit stops responding to system requests for updated signal values, the engine will shut down.

⁸⁶ A momentary failure of the A/D converter that affects the operation of the A/D converter for a short period of time is not expected to have an effect on the operation of the vehicle. This is because the A/D converter digitizes critical signals such as the pedal position signal (VPA1 and VPA2) and the throttle position signal (VTA1 and VTA2) every 1 ms. (VTA1 is converted every 2 ms.). The vehicle's engine will not respond to a momentary failure of the A/D converter that results in erroneous digitization of these signals for a few cycles (i.e. for tens of ms.). This section discusses the possible consequences of abnormal operation of the A/D converter that is sustained for several seconds

- Variations (such as drifts or fluctuations) in the A/D reference voltage will not result in UA.
 - A change in the +5 Vdc signal used by the A/D converter as a reference voltage will also affect the pedal and throttle position signals by the same proportion. Consequently, the A/D converter output will accurately reflect the signals from both the pedal and the throttle.
 - If the variation results in a permanent failure of the A/D converter, the engine will shut down.
- Corruption of the VPA1 and/or VTA1 signal inside the A/D converter (due to, for example, problems in the storage of the digitized values or a failure of the input signal processing circuit) will not result in UA.
 - A fault in the A/D converter which affects only the VPA1 or VTA1 signal will trigger a DTC due to the effective redundancy in the pedal position⁸⁷ and throttle angle⁸⁸ signals.

⁸⁷ DTC P2121, which monitors the relationship between VPA1 and VPA2, will be triggered if the difference between VPA1 and VPA2 due to the corruption exceeds the allowable range. If the corruption in the value of the VPA1 does not trigger DTC P2121, one of the following will occur:

1. If the vehicle is at idle, the vehicle will remain at idle (as the idle flag for the VPA2 value will indicate that the vehicle is at idle).
2. If the vehicle is being driven, the vehicle may either accelerate or decelerate depending upon the value of VPA1. If the vehicle accelerates and the driver releases the pedal, the VPA2 signal will return to the idle value while the VPA1 signal will remain at the corrupted value. If this corrupted value is such that the threshold for DTC P2121 is exceeded, the vehicle will transition to the limp home mode of operation.

In scenario 2, should the driver continue to press the accelerator pedal after VPA1 is corrupted due to the fault condition, the vehicle may either continue to accelerate or decelerate depending upon the value of VPA1. This scenario is not consistent with the reported incidents of unintended acceleration because the driver is still capable of controlling the speed of the vehicle through the accelerator pedal.

⁸⁸ DTC P0121, which monitors the relationship between the VTA1 signal and the VTA2 signal, will be triggered if the difference between VTA1 and VTA2 signals due to the corruption exceeds the allowable range. If the corruption in the value of the VTA1 signal does not trigger DTC P0121, one of the following will occur:

- If the vehicle is at idle, DTC P0121 will be triggered if the corrupted VTA1 signal differs from the non-linearly corrected pedal request by more than 1°..
- If the vehicle is being driven, the fault condition would result in the value of the VTA1 signal not responding accurately to changes in the throttle valve opening angle. This will be detected as a stuck-

- A fault in the A/D converter which affects the conversion of all input signals can result in an erroneous conversion (e.g. raising all signals by a fixed amount). This fault will also result in a similarly erroneous conversion for all other input signals (e.g. VPA2, VTA2, MAF sensor signal, IAT sensor signal, oxygen sensor etc.) Numerous scenarios are possible in this condition: These include:
 - A DTC will be triggered if these erroneous conversions result in a mismatch in the pedal and/or throttle signal voltages (or any other input signals), wherein these signals fall outside their allowable ranges.
 - A DTC may also be triggered if the values from various other sensors in the vehicle (for example the MAF sensor, the oxygen sensor, the IAT sensor etc.) fall outside their allowable range of values. For example,
 - A DTC (P0100) will be triggered if the MAF sensor signal falls below 0.2 V or rises above 4.9 V.⁸⁹
 - A DTC (P0110) may be triggered if the IAT sensor signal falls below 0.18 V or rises above 4.91 V.
 - In the event that the fault in the A/D converter does not trigger a DTC, the corrupted signals will result in a change in engine power which will either lead to sub-optimal engine performance or may result in the engine shutting down altogether. This is because engine operation in a vehicle is managed by a tight control over the air-fuel ratio with inputs from various sensors used to determine the amount of fuel that

throttle condition by the ECM, which will trigger DTC P2111 (throttle stuck open) or DTC P2112 (throttle stuck closed).

⁸⁹ A triggering of these DTCs may not necessarily result in the vehicle transitioning to the fail-safe mode. However, the triggering of these DTCs is not consistent with the reported incidents of unintended acceleration.

must be injected to keep the engine running.⁹⁰ A fault in the A/D converter that affects these signals will result in the Main processor on the ECM incorrectly calculating the amount of fuel required. The resultant change in the air-fuel mixture ratio will determine the vehicle response. Small changes in this ratio will lead to small changes in engine power. On the other hand, large changes in the air-fuel ratio will cause a rapid drop in engine power and may lead to the engine stalling.

As discussed above, a destructive failure or abnormal operation of the A/D converter will either lead to small changes in engine power or more likely will trigger a DTC. DTCs associated with this failure are not consistent with reports on vehicles alleged to have experienced unintended acceleration in the field.

6.8.1.2 A/D Circuit Failure

A failure of the A/D circuit may lead to the following:

- A failure of the A/D converter can either be a result of the failure of the ASIC itself or a failure of a portion of the ASIC. A failure of the circuit will be detected by the Main processor, which will trigger a DTC and transition the vehicle to the fail-safe mode (section 6.1.1.1).
- If the A/D converter circuit fails in isolation, the digitized signal values will deviate from their operating range, triggering a number of DTCs. The diagnostic modules are designed to detect a deviation in the sensor output signals from both the accelerator pedal and the throttle assembly in addition to monitoring the difference between the signals.

⁹⁰ For example, the MAF sensor, the oxygen sensor, etc.

- The consequences of other failures of the A/D converter that lead to abnormal operation of the converter are discussed in section 6.8.1.1.

6.8.1.3 Under-Voltage

Since the A/D converter is powered by the regulated main + 5 Vdc power supply, which also supplies dc power to the Hall Effect sensors (outputs VPA1, VPA2) on the pedal and on the throttle body (outputs VTA, VTA2), any drop in the supply voltage will be reflected on all the signals in a ratiometric manner. If the power supply voltage drops below approximately $\frac{1}{2}$ V, both processors will be reset by the Power Supply IC, causing the vehicle's engine to shut down (section 6.7.3.3).

6.8.1.4 Over-Voltage

Between 5 Vdc and $\frac{1}{2}$ Vdc, the A/D converter will operate normally. An over-voltage condition that exceeds the maximum ratings of $\frac{1}{2}$ Vdc for the Sub processor ASIC, can result in a destructive failure of the IC, causing the engine to shut down and permanently damaging the ECM. However, if the over-voltage condition does not lead to a destructive failure, it can cause the A/D converter to operate abnormally. The response of the vehicle to abnormal operation of the Sub processor due to an over-voltage condition was discussed in section 6.7.3.4. If the Sub processor continues to operate normally and only the A/D converter operates abnormally due to the over-voltage condition, the response of the vehicle will be as discussed in section 6.8.1.1.

6.8.1.5 Over-Temperature

The A/D converter is part of the Sub processor ASIC, which as discussed above, operates within its temperature rating under all operating conditions. If the over-temperature condition causes a failure of the A/D converter, the vehicle will shut down. If, on the other hand, the over-temperature condition causes abnormal operation of the A/D converter, the response of the vehicle will be as discussed in section 6.8.1.1.

For configurations where the A/D converter is located on the Sub processor, an over-temperature condition can affect both the Sub processor and the A/D converter. An over-temperature condition that results in a failure of the A/D converter will also likely cause a failure of the Sub processor. The consequences of the Sub processor failure, as discussed in section 6.1.1.1, will be a transition of the vehicle to the fail-safe mode or a shutdown of the vehicle's engine.

6.8.1.6 Latch-up

If a latch-up condition in the A/D converter were to occur, this may result in abnormal operation of the A/D converter. The vehicle response in the event of abnormal operation of the A/D converter is discussed in section 6.8.1.1. In addition, a latch-up condition can cause the main power supply output voltage to drop to approximately 2 V (section 8.3). Both processors will be reset by the Power Supply IC if the power supply output voltage drops below approximately 3.5 V causing the engine to shut down.

6.8.1.7 Electrical Noise and Transient Over-Voltage

Transients at the input terminals to the A/D are suppressed by a passive pi-filter network for Camry vehicles on each of the input signals, VPA1, VPA2, VTA, VTA2 prior to entering the Sub processor ASIC. Additional on-board filter components suppress any transients on the power supply lines. These medium and high frequency filter capacitors are strategically located to provide additional transient protection. Testing performed by Exponent on the ECM and the entire ETCS-i system for EMI interference did not identify a root cause that would explain the reported incidents of unintended acceleration.

6.8.1.8 Cross-talk

Under certain conditions, cross talk between signals may occur in a multiple power supply distribution system due to parasitic inductive, resistive, or capacitive coupling between the circuits. However, the ECM design uses a single-supply power distribution scheme.

6.8.1.9 Drift in Reference Voltage Signals

A drift in the A/D converter reference voltage signals may affect the operation of the A/D converter. Tests were performed to characterize the response of the vehicle to a drift in the A/D converter reference voltage signals. These tests also simulated a potential corruption of the analog signal due to incorrect digitization of the input signals. Testing was performed on both a 2007 L4 and a 2007 V6 Camry. The testing simulated a fault of both the positive and negative reference voltage supply circuits independently and simultaneously.⁹¹ Three tests were performed:

- Test 1: Fault on Positive Reference Voltage Supply Circuit
 - Negative voltage offset added to reduce the magnitude of the positive reference voltage supply
- Test 2: Fault on Negative Reference Voltage Supply Circuit
 - Positive voltage offset added to increase the magnitude of the negative reference voltage supply
- Test 3: Fault on both Positive and Negative Voltage Supply Circuit
 - Negative voltage offset added to reduce the magnitude of the positive reference voltage supply & positive voltage offset added to increase the magnitude of the negative reference voltage supply

The results of the tests are detailed in Appendix F. DTCs were set for voltage offsets above approximately 0.5 V. For voltage offsets of less than approximately 0.5 V, the maximum engine rpm was recorded below approximately 1600 rpm with the vehicle at idle.⁹² None of the tests performed resulted in a condition consistent with the reported incidents of unintended acceleration.

⁹¹ The tests were run with the vehicle at idle and with the pedal pressed such that VPA1 = 1.0 V before the introduction of the fault.

⁹² No significant increase in vehicle rpm was observed during tests where VPA1 = 1.0 V before the introduction of the fault.

6.8.2 Summary

The ECM design and system protection components ensure that a failure of the A/D converter will trigger a DTC or cause the vehicle's engine to shut down. Exponent could not identify any A/D converter faults that would lead to unintended acceleration.

6.9 Throttle Motor Driver IC

The throttle motor driver IC receives the PWM signals from the Main processor and generates signals to drive the throttle motor and open/close the throttle valve. The throttle motor driver IC, together with the H-bridge (four MOSFETs) generates the signals that control the throttle motor. Most Toyota vehicles equipped with ETCS-i technology (including all Camrys), utilize a system configuration which incorporates two of the four H-bridge MOSFETs in the same IC package as the throttle motor driver IC. Some vehicle designs utilize four external MOSFETs for the H-Bridge. In addition, integrated into the throttle motor driver IC for most Toyota vehicles equipped with ETCS-i technology, is circuitry which receives the trigger pulses for one or more ignition coils. The circuitry in the throttle motor driver IC provides increased drive capability for the trigger pulses. For example in the 2007 V6 Camry, the throttle motor driver IC receives the trigger pulses for four of the six ignition coils from the Main processor.

6.9.1 Principle of H-Bridge Configuration

The throttle motor driver IC drives the throttle valve by controlling the current supplied to the throttle motor through an H-bridge. Figure 88 is a functional diagram of an H-Bridge. The H-bridge consists of four switches (MOSFETs) which control the direction of current to the motor and the movement of the throttle valve. In Figure 88, for clockwise rotation, MOSFETs U1 and U4 are closed, and MOSFETs U3 and U2 are opened. Current from the battery is conducted through MOSFET U1, the motor, and through MOSFET U4 to ground. For counter-clockwise rotation, MOSFETs U1 and U4 are opened while MOSFETs U3 and U2 are closed, with the direction of the motor current reversed.

As an example, in the 2007 V6 Camry, the power stage to the throttle motor has the top two MOSFETs (U1 and U3 in Figure 88) physically located inside the throttle motor driver IC with the bottom two MOSFETs external to the throttle motor driver IC.

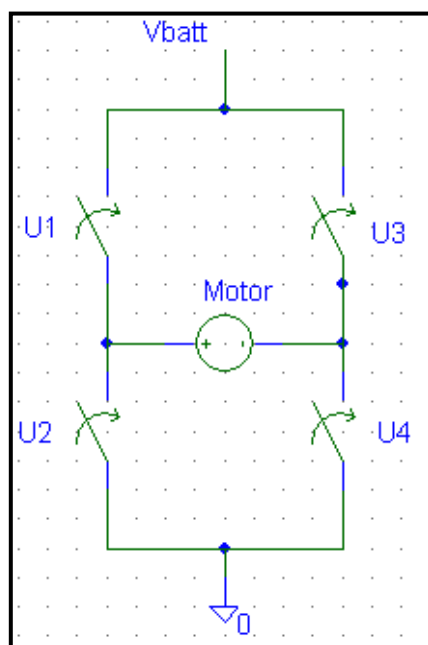


Figure 88. Principle of H-bridge motor drive (U1, U2, U3 and U4 represent MOSFETs in this diagram).

The throttle motor driver IC in all ECMs is constructed using SOI technology, which effectively mitigates latch-up.⁹³ Internally, this IC has a logic section and a power section. The logic section is operated from the main + 5 Vdc supply. The power section operates from the vehicle battery.

6.9.2 Logic Section

The logic section of the throttle motor driver IC controls the PWM pulses to the throttle motor, provides the Main processor with feedback on the status of the throttle motor, and also provides increased drive to the trigger pulses for the ignition coils.

⁹³ Except 2006-2008 Corolla and Matrix ECMs manufactured by Delphi. Latch-up mechanisms in these ECMs are discussed in Appendix C.

6.9.2.1 Power Section

The power section of the throttle motor driver IC boosts the drive capability of the PWM pulses to the throttle motor. An external power MOSFET, controllable by both the Main processor and the Sub processor, is turned off to cut power to the H-bridge when the vehicle transitions to the Class 2 fail-safe mode (section 3.4).

6.9.2.2 Throttle System Monitoring

The throttle motor driver IC monitors various aspects of the throttle motor such as the motor current and voltage, and communicates this information to the processors. The processors use this information for fault detection. The processors can disable⁹⁴ throttle valve control in two ways:

- By sending a signal to the throttle motor driver IC to terminate the drive signals to the motor
- By sending a signal to the throttle motor driver IC to cut the power supply to the H-bridge.

6.9.3 Failure Modes

This section discusses potential failure modes of the throttle motor driver IC and the vehicle response to these failure conditions. The following failure modes will be discussed:

- IC Failure
- Under-voltage
- Over-voltage
- Over-temperature
- Electrical noise and voltage transients

⁹⁴ This would cause the throttle valve to move to the 6° opening angle due to the return springs

- H-bridge transistor failure(s)
- Latch-up.

6.9.3.1 Abnormal Operation

A number of the failure modes listed above can lead to abnormal operation of the throttle motor driver IC. Exponent performed a detailed analysis of the various abnormalities that may be exhibited by the throttle motor driver IC and H-bridge system, and the corresponding vehicle response. The following scenarios are possible:

- Abnormal operation of the throttle motor driver IC may cause the throttle valve to open to an angle inconsistent with the pedal request
 - If the throttle motor driver IC stops responding to commands from the Main processor and opens the throttle valve, the Main processor will try to rectify this condition. If unable to do so, the Main processor will detect this as a stuck throttle condition, triggering either DTC P2111 (throttle stuck open) or DTC P2112 (throttle stuck close) and transitioning the vehicle to the fail-safe mode.
 - If the throttle motor driver IC incorrectly interprets the throttle opening request from the Main processor, it may open the throttle to a different angle than that requested by the Main processor. In this condition, the Main processor, using feedback from the sensors in the throttle assembly, will try to bring the throttle valve back to the correct opening angle. One of several DTCs (P2111, P2112, P2121) will be triggered if the Main processor is unable to bring the throttle valve to the desired opening angle.
 - DTC P2119 will also be triggered (by the Sub processor) if the throttle opening angle exceeds the non-linearly corrected pedal request by approximately 3° when the vehicle is at idle or approximately 25° when the vehicle is being driven (section

7.9.2). In the event that the throttle opening angle due to this failure exceeds the non-linearly corrected pedal request by more than 3° but less than approximately 25°, the throttle valve will be opened to the incorrectly calculated angle. However, as soon as the vehicle starts to accelerate (due to this fault condition), the expected driver response will be to release the pedal, slowing down the vehicle and transitioning it to the idle mode (where a DTC is triggered, if the throttle opening angle exceeds the non-linearly corrected pedal request by approximately 3°).

- If the circuit in the throttle motor driver IC that generates the trigger pulses for the ignition coils⁹⁵ starts to operate abnormally, the timing of the ignition pulses may be affected. Any change in the timing of the ignition pulses will cause the vehicle's engine to operate in suboptimal fashion or to shut down.

6.9.3.2 IC Failure

A failure of the throttle motor driver IC due to a defect in a chip or due to external stresses may lead to a termination of the trigger pulses for the ignition coils. This condition will cause the vehicle's engine to shut down. In addition, a failure of this IC will trigger numerous DTCs (such as stuck throttle condition DTCs etc.), which will transition the vehicle to the fail-safe mode.

6.9.3.3 Under-Voltage

The throttle motor driver IC has an under-voltage lock-out which activates if the voltage drops below approximately 2.7 V. The throttle motor driver IC is powered by the same +5 Vdc power supply that powers the processors and sensors, including the throttle position and pedal position sensors. The system design ensures that the processors are reset if the power supply voltage drops below approximately 3.5 V. Hence, even though the throttle motor driver IC has an under-

⁹⁵ Four of the six trigger pulses in the 2007 V6 Camry.

voltage lockout, the system design ensures that the vehicle's engine will shut down before the voltage drops to the value which will trigger the under-voltage lockout mechanism on this IC.

6.9.3.4 Over-Voltage

A voltage output exceeding +5 V will affect all components powered by the power supply. Similar to the voltage rating of the processors (section 6.7.3.4), the throttle motor driver IC logic circuitry is also rated for operation to V_{dc} . Hence, the operation of the throttle motor driver IC will not be affected for a power supply voltage up to V_{dc} . A power supply IC voltage exceeding V_{dc} would likely be a consequence of a failure of the power supply IC, which would likely be permanent and detectable after the incident.⁹⁶

However, if the failure of the power supply is not permanent and leads to a voltage that exceeds the absolute maximum voltage rating of the throttle motor driver IC, the IC may operate abnormally. The vehicle response to the abnormal operation of the throttle motor driver IC is discussed in section 6.9.3.1.

6.9.3.5 Over-Temperature

The throttle motor driver IC on Camry vehicles is manufactured using Silicon-on-Insulator (SOI) technology which enhances the high temperature and high voltage performance of the IC. Test data reviewed by Exponent indicates that the throttle motor driver IC and the H-bridge transistors operate within their rating for temperature under real world operating conditions with adequate temperature de-rating designed into the system. Although the analysis and document review performed by Exponent does not provide any indication of the throttle motor driver IC or the H-bridge transistors failing due to an over-temperature condition, temperatures that are outside the rating may cause them to fail or function incorrectly. This will not lead to UA.

⁹⁶ In addition, this condition would likely lead to a failure of the processors and/or the throttle motor driver IC.

6.9.3.6 Electrical Noise and Voltage Transients

Multiple protection components protect the throttle motor driver IC and associated circuitry from external noise sources. In addition, testing performed by Exponent on the ECM and the entire ETCS-i system did not identify a root cause that would explain the reported incidents of unintended acceleration.

6.9.3.7 H-Bridge Transistor Failure(s)

The following scenarios are possible:

- An open-circuit failure of one or more transistors will lead to an inoperable throttle valve.
- In the event of a short circuit failure of one or more transistors, a number of scenarios are possible from a short circuit of the battery terminals to a stalling of the throttle motor. These conditions will trigger the motor over-current fail-safe and/or result in permanent damage, such as an open fuse or damage to one or more components, and the traces on the ECM circuit board may result. This damage would be visible after the incident.

Failures of one or more transistors of the H-bridge cannot explain the reported incidents of unintended acceleration.

6.9.3.8 Latch-up

A latch-up of the throttle motor driver IC or the H-bridge can lead to a wide open throttle condition. However, the throttle motor driver ICs are manufactured using SOI technology. This technology is an effective mitigation mechanism against latch-up. In addition, the throttle motor driver IC is tested in accordance with industry standard JEDEC /JESD78: “IC Latch-Up Test” to ensure that the IC is not susceptible to latch-up.

Even in the unrealistic scenario of a latch-up condition on the throttle motor driver IC or the associated H-bridge, the system response will be either a transition to the fail-safe mode or a shut-down of the vehicle's engine. The following items will be addressed to develop the analysis to show that a latch-up condition, whether selective latch-up or full latch-up, does not result in unintended and uncontrolled throttle motor operation and throttle motor opening. The following latch-up conditions are considered:

1. Selective latch-up where the Main and Sub processors have control of the throttle motor driver IC which is still functional; however, for example MOSFETs U1 and U4 are latched on (Figure 88)
2. Full latch-up where all four MOSFETs, U1-U4 (Figure 88) are latched on⁹⁷
3. A latch-up condition which leads to abnormal operation of the throttle motor driver IC.

Various fail-safes designed into the system will detect the latch-up condition and transition the vehicle to the fail-safe mode during both selective and full latch-up. These include:

- Throttle valve stuck condition (DTC P2111/P2112)
 - These DTCs are triggered due to a stuck throttle (stuck open or stuck closed) condition and are triggered if all of the following conditions occur for 500 ms.:
 - a. Measured motor current $> 2\text{ A}$
 - b. The change in VTA1 is less than a predetermined threshold
 - c. PWM duty cycle to open/close throttle is $> 80\%$

⁹⁷ In this instance, no current will flow through the throttle motor. The throttle valve will return to the 6° position.

- If a latch-up causes a wide open throttle condition:
 - The throttle valve will be stuck at the wide open position (84°) and the current through the throttle motor will be higher than 2 A due to the wide open position (this will trigger condition ‘a’ above).
 - In addition, because the throttle position will not change due to latch-up, this will trigger condition ‘b’ above
 - Since the throttle valve opening angle reported by the throttle position sensors will be higher than the throttle valve opening instruction value, the Main processor will try to close the throttle valve. However, the throttle valve will not respond (close) due to the latch-up condition. The Main processor will increase the PWM duty cycle as it tries to close the throttle valve. The duty cycle will rise above 80% in approximately 4-5 cycles. This will trigger condition ‘c’ above.
 - All three conditions (‘a’, ‘b’ and ‘c’) will remain triggered due to the latch-up condition. 500 ms. after all three conditions are triggered, DTC P2111 will be set.
 - The processor will try to close the throttle to fail-safe position (6°). However, the latch-up condition will prevent the throttle from moving. The air flow detected by the mass air flow sensor will exceed the calculated air flow, which will cut the fuel to the engine and cause the engine to shut down.
- Motor Over-Current Condition (DTC P2103)
 - A latch-up condition that leads to a wide open throttle condition will cause a large current to be continuously conducted by the motor. The system is designed to detect this

occurrence as a fault and trigger a DTC, transitioning the vehicle to the fail-safe mode.

- The Main processor will try to close the throttle to fail-safe position (6°). However, the latch-up condition will prevent the throttle from moving. The air flow detected by the mass air flow sensor will exceed the calculated air flow, which will cut the fuel to the engine and cause the engine to shut down.
- System Guards (DTC P2119)
 - The functionality of the system guard modules is described in detail in section 8.4. A latch-up condition leading to a stuck throttle condition will cause the triggering of one or more of the system guard modules due to the deviation of the throttle opening angle from the calculated position as based on the driver request. This will lead to a fail-safe mode of operation.
 - A latch-up that creates a short circuit at the power supply could lead to the power supply output voltage dropping to approximately 2 V.⁹⁸ As discussed in section 6.6.3.3, this will cause both processors to be reset and lead to the vehicle's engine shutting down.
- The consequences of abnormal operation of the throttle motor driver IC due to a latch-up condition are discussed in detail in section 6.9.3.1.

6.9.4 Summary

Exponent's testing and analysis has identified no failures of the throttle motor IC and the associated circuitry (H-bridge) that would lead to UA. Testing and analysis performed indicates that:

⁹⁸ "Latch-up", Steven H. Voldman, John Wiley & Sons Ltd., 2007, pp. 225

- The filter circuit used on the throttle motor driver circuit provides adequate protection against external noise and other EMI sources.
- A latch-up condition is not realistic due to the use of SOI technology. However, if a latch-up condition did occur, a DTC would be triggered, cause the engine to shut down, and potentially cause permanent damage to the ECM.
- All other potential failure modes lead to the vehicle either operating normally or the vehicle's engine shutting down preventing UA.

Exponent could not identify any realistic faults of the throttle motor driver IC and related circuitry that could reasonably explain the reported incidents of unintended acceleration.

6.10 Summary

Exponent's analysis of the ECM hardware and its functionality indicated the following:

- The ECM is designed to constantly monitor the operation of processors in the ECM. A failure of either of the Main processor or the Sub processor results in a resetting of the processors which causes the vehicle's engine to shut down.
- An analysis of the Main processor and the Sub processor design and the results of the testing performed indicate that there are no fault conditions of the processors which can cause the vehicle to experience UA.
- Several hypothesized failure modes were considered for the different components, including failure modes mitigated by the use of SOI technology. Exponent's testing and analysis has identified no failures that would lead to UA.

- Testing and analysis indicate that if failures such as latch-up were to occur, the system will transition the vehicle to the fail-safe mode or cause the vehicle's engine to shut down altogether.
- The system design ensures that any failure of the throttle motor driver IC and/or its associated circuitry (H-bridge) will cause the vehicle to either transition to the fail-safe mode or result in the vehicle's engine shutting down.

The analysis in this chapter was directed to understanding how the ECM would respond to stresses arising from abnormal conditions such as over-voltage, over temperature, latch-up etc. As part of its analysis, Exponent also reviewed the data on reported complaints of unintended acceleration to identify whether certain environmental or operating conditions or incident descriptions would be consistent with development of over-temperature or over-voltage conditions. For example, the data were analyzed to identify whether incidents occurred predominantly in hot conditions or under high load conditions, or whether other problems that would result as a consequence of the abnormal conditions (such as DTC codes, permanent damage, etc.) were described in conjunction with the reported unintended acceleration events. No such patterns were identified in the data, further supporting the findings that these abnormal conditions were not factors that could reasonably explain the reported incidents of unintended acceleration.

Based on the review, analysis and testing performed of Toyota Camry vehicles equipped with ETCS-i, Exponent has been unable to identify any hardware related faults or mechanisms on their ECMs that could explain the reported incidents of unintended acceleration.

7 ECM Software

7.1 Introduction

The vehicle response depends on the interaction of several vehicle systems in addition to the driver and the driving conditions. The software that resides in the ECM is one of the components that was analyzed by Exponent. Exponent's review focused on the ECM software that was related to the ETCS-i system on Camry vehicles. The Camry vehicle software has had three changes since the introduction of ETCS-i in 2002. These changes occurred in 2002, 2004 and 2007 model year vehicles. For this reason the software analysis was focused on reviewing the source code from these three model years. The changes in the software architecture were necessitated due to regulatory requirements (for example, mandatory requirements set by the California Air Resources Board (CARB)) and due to hardware changes. This chapter details the software analysis performed by Exponent as part of this investigation. It is important to understand that due to the inherent nature of the interaction between the software and the vehicle in an ETCS-i equipped vehicle, the software system cannot be analyzed in isolation. The analysis must consider the vehicle's behavior in characterizing the effect of any hypothesized software system failure.

7.2 Approach

A systematic approach was taken to fully understand and analyze the ETCS-i related software system of a chosen Toyota vehicle model and based on the understanding of the model's software system, compare it to the software system of other models to analyze the consequences of the identified differences on UA. The software system of the 2007 V6 Camry was chosen as a starting point for the software review. Figure 89 gives a high level overview of the approach taken.

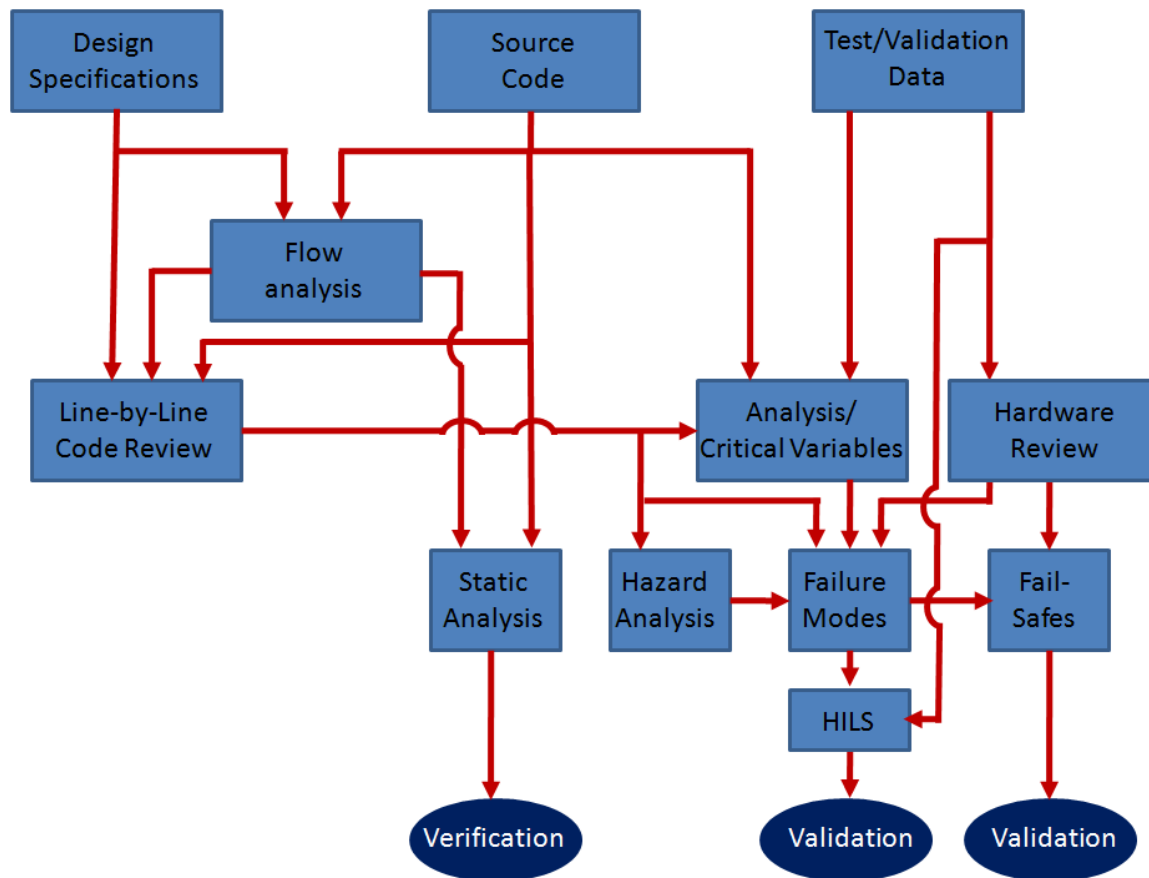


Figure 89. Approach to software analysis.

The analysis focused on understanding the throttle control and fail-safe algorithms to identify failure modes and analyze the system response to these failure modes. These identified failure modes were then tested by using either the hardware in the loop simulator (HILS) or, if possible, on vehicles to determine the system response to the identified failures. The following analysis was performed:

- Review of the design and specifications for the 2007 V6 Camry. This included a review of the coding rules, test procedures etc. employed by Toyota.
- A flow analysis to understand the inter-linking of the various modules involved in throttle control and the flow of information between the modules

- A line-by-line review of the source code to analyze:
 - The operation of modules involved in throttle control. This enabled the development of an understanding of the operation of the throttle control algorithm and aided in defining the bounds on critical variables and the effect of a failure of one or more modules on the throttle valve position.
 - The operation of the numerous fail-safes in the software. The analysis of the software fail-safes was used to determine whether failure modes identified (both in the vehicle's hardware and software) could lead to UA.
- Static analysis to verify the software system's operation per its specification and to identify any sources of real time error that could affect throttle valve position.
- Hardware in the loop simulation (HILS) to characterize the system response to the identified failure modes.
- A detailed review of all the software test data and validation reports to understand the testing performed on the software and to complement the results of Exponent's analysis of the source code.

Once the analysis of the source code for the 2007 V6 Camry had been completed, Exponent studied the software of other Toyota vehicles. The aim of this study was to understand the differences in the throttle control software architecture between the other vehicles and the 2007 V6 Camry and to analyze the effects of these differences on throttle control and UA. This chapter will detail some of the analysis performed on the software of Toyota Camry vehicles equipped with ETCS-i.

7.3 Flow Review

The interconnection between modules involved in throttle control and the flow of information from one module to another was analyzed to understand system operation and software architecture. A flow analysis was performed for the 2002 V6 Camry, the 2004 L4 Camry and the 2007 V6 Camry. Exponent used custom-developed and off-the-shelf automated analysis tools for this purpose. Scripts using both Python and Shell were written to generate data for creating the flow diagrams.

The inter-relationships between the throttle control related modules identified by Exponent were used as a starting point in the analysis of the source code. The flow diagram generated a set of modules of interest for the line-by-line code analysis. The aim of the line-by-line source code review was to determine several aspects of module behavior which included the operation of the modules, how the modules controlled the throttle opening angle, the operation of the diagnostic modules, the absolute limits on throttle opening request from the various modules, etc.

7.4 Static Analysis

Static analysis generally refers to automated methods that facilitate the detection of run-time errors without the actual execution of the code. The main purpose of static analysis is to detect any unexpected run time events that may cause the program execution to prematurely abort or result in undesirable behavior by the software. Examples of run time errors which can typically be detected by static analysis include resource leaks (i.e. improper resource allocation), illegal operations (e.g. variable or buffer overflow), incomplete code, non-termination of loops, etc.⁹⁹

Exponent used PolySpace[®] (release R2010a), an industry accepted software verification tool from Mathworks, Inc., for the static analysis. The source code of the 2002 V6 Camry and the 2007 V6 Camry was analyzed using PolySpace[®].

⁹⁹ Pär Emanuelsson & Ulf Nilsson, "A Comparative Study of Industrial Static Analysis Tools", Technical reports in Computer and Information Science, Report Number 2008:3

7.4.1 Module Selection

For analyzing the source code of the selected vehicles, the primary modules that have an influence on the calculation of the throttle angle were selected. The documentation reviewed by Exponent and the flow analysis performed on the source code identified the modules that have an influence on the calculation of the throttle angle.

7.4.2 PolySpace® Results

PolySpace® returns four types of status for each code segment analyzed. The following status indications are returned by PolySpace®:

- Red: This indicates a “Proven Run-Time Violation”
- Gray: This indicates a “Proven Unreachable Code Branch
- Orange: This indicates an “Unproven Run-Time Check”
- Green: This indicates that the code is proven not to contain any run-time errors at the language level.

7.4.3 2002 V6 Camry

7.4.3.1 Processing Order

Each module includes various function calls that are made to perform a certain task. These modules are called by the operating system in a specific order. A main file was written to:

- Enable PolySpace® to exercise all functions of the analyzed modules.
- Ensure the same order of processing for the modules during the static analysis as during actual code execution in the vehicle. This ensured that when global variables were used to communicate between modules, the

modules that set or initialized the global variables were called before the module that used the variable's stored value.

7.4.3.2 PolySpace® Results

Table 10 below summarizes the results of the PolySpace analysis on the primary throttle control modules analyzed for the 2002 V6 Camry source code.

Table 10. 2002 V6 Camry primary throttle modules code verification summary

Code Verification	
PolySpace Verifier	Enabled
Number of Result Sets	x 1
Reds	0
Grays	101
Oranges	147
Green	3654
Proven	96.2%
Pass/Fail	

Table 10 shows the following:

- 96.26 % of the code in the analyzed modules does not contain any run-time errors at the language level.
- There were 101 locations of unreachable code identified by PolySpace®. Each of these locations was analyzed and deemed not to be of concern. The majority of these locations were due to the use of macros for consistent conversions with constants, and limit checks on previously set values. Each of these locations was reviewed to determine why they were flagged as unreachable by PolySpace®. A number of these instances were due to bound checks that were performed in the source code. These were unreachable because they involve values that cannot be reached within the logic of the

code. These bounds checks provide additional safety, but PolySpace was not able to verify them, as they could only apply with values that PolySpace believes are impossible.

- There were 147 locations of unproven run time checks identified by PolySpace® in the modules. Each of these was reviewed and determined to be safe and not to result in run-time errors.

7.4.4 2007 V6 Camry

7.4.4.1 Module Selection

The static analysis performed using PolySpace® on the 2007 V6 Camry was divided into two runs:

- **Primary Throttle Modules:** In this analysis, the focus was on reviewing and analyzing the modules that have an influence on the calculation of the throttle angle
- **Idle Speed Control Modules:** In this analysis, the focus was on reviewing and analyzing electrical loads and other systems of the vehicle which may influence the throttle opening angle.

7.4.4.2 Primary Throttle Modules

The documentation reviewed by Exponent and the flow analysis performed on the source code for the 2007 V6 Camry identified the modules that have an influence on the calculation of the throttle angle.

7.4.4.3 Idle Speed Control

The idle speed control (ISC) module is used as an input for the determination of the throttle opening position along with the primary throttle modules. The documentation reviewed by

Exponent and the flow analysis performed on the source code identified the modules that are used as inputs into the idle speed control (ISC) module. That list, with some modifications, was used as the input for another PolySpace[®] run.

7.4.4.4 Processing Order

As with the 2002 V6 Camry source code, a main file in the C programming language for both PolySpace runs was written.

7.4.4.5 Primary Throttle Modules

For the first PolySpace[®] run performed on the primary throttle modules, the main file was used by PolySpace[®] to determine the order for analysis of the included functions. This restricted the values of certain variables and provided more accuracy for the analysis.

7.4.4.6 Idle Speed Control Modules

Similar to the main file written for the analyses of the primary throttle modules, a main file for the idle speed control modules provided PolySpace[®] with the order of the modules for the analysis.

7.4.4.7 Primary Throttle Modules

Table 11 below summarizes the results of the PolySpace[®] analysis on the primary throttle control modules.

Table 11. 2007 V6 Camry primary throttle modules code verification summary

Code Verification	
PolySpace Verifier	Enabled
Number of Result Sets	x 1
Reds	0
Grays	285
Oranges	80
Green	5154
Proven	98.6%
Pass/Fail	

Table 11 shows the following:

- 98.6 % of the code in the analyzed throttle modules does not contain any run-time errors at the language level.
- There were 285 locations of unreachable code locations identified by PolySpace[®]. Each of these locations was analyzed and deemed not to be of concern. The majority of these were due to the use of macros for consistent conversions being used with constants, and limit checks on previously set values.
- There were 80 locations of unproven run time checks identified by PolySpace[®] in the modules. Each of these was reviewed and determined to be safe and not to result in run-time errors.

7.4.4.8 Idle Speed Control

Table 12 summarizes the results of the PolySpace[®] analysis on the idle speed control modules.

Table 12. 2007 V6 Camry PolySpace® ISC code verification summary

Code Verification	
PolySpace Verifier	Enabled
Number of Result Sets	x 1
Reds	0
Grays	361
Oranges	98
Green	5605
Proven	98.4%
Pass/Fail	

Table 12 shows the following:

- 98.4 % of the code in the analyzed idle speed control modules does not contain any run-time errors at the language level
- There were 361 locations of unreachable code identified by PolySpace®. Each of these locations was analyzed and deemed not to be of concern. The majority of these were due to the use of macros for consistent conversions being used with constants, and limit checks on previously set values.
- There were 98 locations of unproven run time checks identified by PolySpace® in the modules. Each of these was reviewed and determined to be safe and not to result in run-time errors.

7.4.5 Summary

Exponent performed a static analysis on selected modules from the source code for the 2002 V6 Camry and the 2007 V6 Camry using PolySpace®. The modules selected for both vehicles belonged to sections of the source code that directly or indirectly influence the throttle opening angle. The findings from PolySpace® were:

- 4000 checks on the analyzed modules for the 2002 V6 Camry were unable to conclusively determine the absence of run-time errors in 147 locations. These locations were reviewed and determined not to result in run-time errors.
- 11500 checks on the analyzed modules for the 2007 V6 Camry were unable to conclusively determine the absence of run-time errors on 178 locations in the analyzed modules. These locations were reviewed and determined not to result in run-time errors.

Exponent manually reviewed the code to determine whether any of the unresolved locations identified by PolySpace[®] could give rise to run time errors. Exponent was able to eliminate all PolySpace[®] unresolved locations in the analyzed modules as sources of run-time errors. The PolySpace[®] analysis indicates that on the modules analyzed and in the context in which the modules were analyzed, there are no run time errors at the language level. In addition, Exponent's manual review of the code along with the results obtained using PolySpace[®] did not identify any run-time errors at the language level on the analyzed modules that may lead to unintended acceleration.

7.5 Mirroring

In addition to performing extensive checks on the various sensor input signals to ensure that the signals are within bounds, the software is designed so that critical variables (for example the non-linear pedal request, the throttle opening request, etc.) are mirrored. Mirroring involves the following:

- When a critical variable is being saved in memory (SRAM storage), a copy of the variable in which all the bits have been inverted is also saved.
- When the critical variable is being read from memory for processing, the mirrored image of the variable is also read from memory. The bits of the mirrored image are flipped and the result is compared with the variable itself.

Any deviation in the image and the variable itself is flagged as a memory failure and results in a DTC (P0604 for a 2007 V6 Camry).¹⁰⁰ This triggers a Class 2 failure which transitions the vehicle to the fail-safe mode.

The mirroring of critical variables increases detects the corruption of memory and prevents this corruption from causing unintended throttle opening.

7.6 Error Correction Code (ECC)

Exponent performed a detailed review of the ICs and the memory used for storing information and programs in the ECM. Exponent's analysis to date indicates that the use of ECC corrects 1 bit per byte in both the ECM's Main processor RAM and ROM. When an error is detected, the data output will be corrected by the ECC code. In addition to ECC, the Main CPU in the ECM also mirrors critical variables used to determine throttle opening angle and can detect when a RAM error causes corruption of these variables. This is done by creating a mirror value (by flipping bits) of calculated variables immediately after the global variable value is assigned. The mirror values are checked against the retrieved values from RAM, and a DTC is triggered if an error is detected. This technique has the ability to detect rare events, such as errors on multiple bits.

7.7 Resource Locking

Resource locking occurs when multiple modules on a processor try to access resources simultaneously. There is no shared hardware between the Main processor and the Sub processor. Hence, if a resource lock were to occur on one processor, hardware watchdogs, and monitoring of the processor idle times would detect such a condition if it exceeded acceptable limits, and would transition the vehicle to a fail-safe mode.

¹⁰⁰ DTC triggered within 2 seconds of the fault being detected by the ECM.

7.8 Test Data/Validation Report Review

Exponent also reviewed the software test reports provided by Toyota as part of the software analysis. Test documentation reviewed included:

- Modified Condition/Decision Coverage (MC/DC) test reports
- Static test reports including reports generated using the following tools:
 - C-Checker
 - QA-C (A deep flow static analysis tool)
 - CAST
- Dynamic test reports
- Task interference test reports
- Other software reports.

Exponent did not identify any scenario through a review of the test reports that could explain the alleged incidents of unintended acceleration.

7.9 Hardware-in-the-Loop Simulation

As part of the analysis of the source code, Exponent generated test vectors and studied the system/software response to these generated test vectors under both normal and fault conditions. The dynamic analysis was performed using a tool that was developed to verify the response of the ECM and its associated executable program to a set of inputs. Testing was performed on the ECMs of the following two Camry vehicle models:

- 2007 V6
- 2004 L4.

The tool used by Exponent is a proprietary simulator designed and developed by Denso specifically for the purpose of testing Toyota vehicle ECMs. The simulator is connected to an ECM and provides inputs to the ECM. In addition to providing the ability to simulate vehicle response to various input test vectors, the simulator also provides the ability to:

- Simulate sensor signal outputs.
- Analyze actuator signals.
- Simulate the controller area network (CAN) communication signals.
- Debug and analyze the system response in real time.
- Probe the software and inspect the state of critical variables in real time. This functionality enabled Exponent to characterize and study the software system response to better understand and analyze the operation of the ECM control system.

7.9.1 Input Variables

For each of the test runs performed, the vehicle conditions needed to be set before the start of the simulation. The variables in Table 13 were varied and controlled during the simulation runs performed.

Table 13. Variables set at startup

Variable	Description
VG	Airflow meter
+B	Battery voltage (V)
SPD	Vehicle speed (km/h)
NE	Engine RPM
D	Drive mode
STA	Starter signal
STP	Stop lamp switch
ST1-	Brake system
THA	Air temperature (°C)
THW	Water/coolant temperature (°C)

The following settings were also configured prior to performing testing using the simulator:

- ECM information (for example type of signals to use etc.)
- Engine revolution pattern information
- Physical sensor values (these values need to be converted from hexadecimal into physical values for the sensors)
- RAM information
- Fuel to air ratios.

7.9.2 Tests performed

This section presents results from selected test runs performed on a 2007 V6 Camry and a 2004 L4 Camry.

Test 1: Throttle opening angle as a function of pedal depression at ignition on¹⁰¹

The aim of this test was to understand the pedal position learning algorithm and characterize the vehicle response to different pedal positions at ignition on.

Testing indicated that the throttle opening request was a direct function of the pedal position sensor voltage at ignition on regardless of the values learned at ignition on. The test was performed for VPA1 at 0.4V, 0.8V and 1.6V at ignition on. Testing also indicated that with VPA1 at 1.6 V, no pedal position learning occurred and the default (VPA1 = 0.8 V) or previously learned value was used.

Test 2: System response to demands from the Vehicle Stability Control Computer (VSC)¹⁰²

The aim of this test was to characterize system response to an incorrect and large throttle opening request from the VSC computer. The VSC computer, along with the ECT computer,

¹⁰¹ This test was performed on the source code for both model year vehicles.

¹⁰² This test was performed on the source code for both model year vehicles.

can request small changes in the throttle opening angle under certain operating conditions. However, these values are bounded and cannot exceed a few degrees. The aim of this test was to simulate a failure of the VSC computer and/or the module where the demand from the VSC computer was checked and bounded. Testing indicated that:

- A DTC (P2119) was set if the demand from the VSC computer exceeded:
 - 3° when the vehicle was at idle (VPA1 = 0.8 V)
 - 25° when the vehicle was being driven (VPA1 = 1.6 V).¹⁰³

Testing indicates that if the vehicle is being driven, a fault in the VSC system may increase the throttle valve opening angle by up to 25° before a DTC is triggered. However, as soon as the vehicle starts to accelerate, the expected driver response will be to release the pedal, which will transition the vehicle to the idle mode (where a DTC is triggered, if the VSC throttle opening request exceeds approximately 3°). This will trigger a DTC (P2119) transitioning the vehicle to the fail-safe mode.

Test 3: System response to demands from the Idle Speed Control (ISC) System¹⁰⁴

In addition to the request from the driver (pedal/cruise control request), the throttle opening angle is determined by the request from the ISC system, as well as the demands from the various electrical loads in the vehicle. A review of the source code indicated that the maximum demand for the throttle opening angle from all the electrical loads in the 2007 V6 Camry could not exceed 15.5°. A further bound in the source code limited the maximum allowable throttle opening request from the ISC to 15.5°. The aim of this test was to characterize the operation of the ISC system. Testing indicated that the system limited the throttle opening demand to less than 15.5° under all simulated electrical load fault conditions.

¹⁰³ This test run was performed with the idle speed request set to 15°

¹⁰⁴ This test was performed on the source code of both the 2004 and the 2007 Camry.

Test 4: System response to demands from the Electronically Controlled Transmission (ECT) computer¹⁰⁵

The aim of this test was to characterize system response to an incorrect and large throttle opening request from the ECT computer. The ECT computer, along with the VSC computer, can request small changes in the throttle opening angle when activated and under certain vehicle operating conditions. However, these values are bounded and cannot exceed a few degrees. The aim of this test was to simulate a failure of the ECT computer and/or the module where the demand from the ECT computer was checked and bounded. Testing indicated that:

- A DTC (P2119) was set if the demand from the ECT computer exceeded:
 - 3° when the vehicle was at idle (VPA1 = 0.8 V)
 - 25° when the vehicle was being driven (VPA1 = 1.6 V).¹⁰⁶

Testing indicates that if the vehicle is being driven, a fault in the ECT system may increase the throttle valve opening angle by up to 25° before a DTC is triggered. However, as soon as the vehicle starts to accelerate, the expected driver response will be to release the pedal, which will transition the vehicle to the idle mode (where a DTC is triggered, if the ECT throttle opening request exceeds approximately 3°). This will trigger a DTC (P2119) transitioning the vehicle to the fail-safe mode.

Test 5: Resistance in series with supply voltage for throttle position sensors¹⁰⁷

A fall in the voltage of this power supply could affect the output signal from the throttle sensors, providing incorrect information to the ECM regarding the throttle opening angle. Extensive hardware testing was performed to simulate the system response to this scenario. The aim of this test was to validate the hardware testing performed and to characterize and study the ECM algorithm's response to this failure scenario. Testing validated Exponent's understanding of the throttle control architecture and also validated the results of the hardware testing (section 5.5.5).

¹⁰⁵ Since the source code for the manipulation of the signals from the ECT is identical for both model year vehicles, this test was only performed on the source code for the 2007 V6 Camry.

¹⁰⁶ This test run was performed with the idle speed request set to 15°

¹⁰⁷ Since the same throttle position sensor processing algorithms are used for both model year vehicles, this test was only performed on the source code for the 2007 V6 Camry.

Test 6: Resistive fault in series between throttle position sensors and ECM¹⁰⁸

The aim of this test was to characterize the response of the ECM and the PID controller to a resistive fault in series with the feedback signals from the two throttle sensors. Testing indicated that:

- As expected, the introduction of a constant negative voltage offset in the feedback signals from the two throttle sensors resulted in an increase in the throttle valve opening with all other input conditions remaining unchanged
- A negative voltage offset with a threshold ranging from less than 600 mV to approximately 650 mV triggered a DTC (P0121 – due to the throttle position sensor values deviating from their expected values) and transitioned the vehicle to the fail-safe mode
- A DTC (P0121) was triggered for negative voltage offsets of approximately 600 mV or less, when these offsets were introduced into the circuit before the vehicle ignition was turned on
- Variations were observed in the throttle opening angle for a voltage offset of approximately -400 mV due to the PID controller variables resetting and trying to stabilize the throttle motor to its final opening angle.

Test 7: Bit flip errors¹⁰⁹

Error correcting codes (ECC) implemented in the random access memory (RAM) are designed to detect and correct certain errors, such as bit flips. These codes are designed to detect and protect against the introduction of errors on one or more bits in a variable stored in RAM. The aim of this test was to characterize the system response to multiple bit flips that could not be detected by the ECC. The effect of bit flips on critical variables that directly influence the throttle opening angle was investigated as part of this test. As an example, testing was performed to simulate bit flip errors on the throttle opening request signal by introducing a

¹⁰⁸ This test was performed on the source code for both model year vehicles.

¹⁰⁹ This test was performed on the source code for both model year vehicles.

constant offset in the signal to simulate the change in the value of this variable due to undetected bit-flips.

Testing indicated that multiple bit flips can cause a nominal increase in the throttle opening request signal from the ECM to the throttle motor. However, if this increase exceeded 3° , the ECM set a DTC (DTC P2119) transitioning the vehicle to the fail-safe mode for both vehicles.

Should multiple bit flips increase the throttle valve opening angle by less than 3° , a DTC may not be triggered and the vehicle may start to accelerate. However, as soon as the vehicle starts to accelerate, the expected driver response will be to release the pedal, which will transition the vehicle to the idle mode (where a DTC is triggered, if the throttle opening angle exceeds the throttle opening request by approximately 3°). This will trigger a DTC (P2119) transitioning the vehicle to the fail-safe mode.

Test 8: System guard validation¹¹⁰

The aim of this test was to validate the operation of the system level checks and to determine the response of the ECM to various simulated fault conditions that would be expected to trigger one or more of the system level checks. Testing indicated that the system guard module detected a variation between the expected throttle opening angle and the actual throttle opening angle, transitioning the vehicle to the fail-safe mode if the difference between the two exceeded 3° while the vehicle was being driven and exceeded approximately 3° when the vehicle was at idle.

Test 9: VPA1/VTa1 characterization

The aim of this test was to understand the software algorithm ‘learning’ process at ignition on and what effect the signal from the pedal position sensor at “ignition on” had on throttle opening position during vehicle operation. In addition, the test was designed to compare the results obtained from the simulator with results that were obtained on vehicle tests performed on a 2007 V6 Camry.

¹¹⁰ The system guard modules are identical in both the 2004 and 2007 model year vehicles. For this reason, this test was only performed on the source code for the 2007 V6 Camry.

Testing showed that the learned values observed during the HILS testing were comparable with testing that was performed on an actual vehicle.¹¹¹

Test 10: Stuck throttle test¹¹²

The aim of this test was to characterize the response of the vehicle to a stuck throttle condition. One or more DTCs were set for every test condition simulated, indicating that the system is designed to detect any stuck throttle condition in the vehicle and transition the vehicle into the fail-safe mode on the detection of this condition.

7.9.3 Summary

A large number of tests were performed using the simulator. Only a subset of those are presented in this section. Testing performed indicated that:

- If the throttle opening demand from either the VSC or the ECT system exceeds 3° while the vehicle is at idle, the ECM detects this as a fault and transitions to the fail-safe mode. This limit was observed to be 25° when the vehicle was being driven. However, if a VSC or ECT system failure occurs when the vehicle is being driven, and the driver releases the accelerator pedal, the vehicle transitions to the idle mode, which would trigger the 3° condition. Testing using HILS allowed for the elimination of a failure of either the VSC or the ECT sub-system as a realistic explanation for the reported incidents of unintended acceleration.
- A large number of tests were performed to study and understand the idle pedal position learning algorithm. The results of these tests helped with the development of specific test conditions when evaluating the consequences of resistive faults in accelerator pedal circuits.

¹¹¹ A small deviation was observed due to the deviation in the Hall Effect output signals on the vehicle from their default values (VPA1 = 0.8 V and VPA2 = 1.6 V) assumed in the simulation

¹¹² Since the module responsible for this functionality was identical between the 2004 L4 Camry and the 2007 V6 Camry, the test was only performed on the source code of the 2004 L4 Camry.

- The tests simulating simultaneous resistive faults on both throttle position circuit outputs allowed for the determination of the bounds on the faults that could exist without the triggering DTCs. In addition, the tests also aided in the evaluation of the PID control system to characterize the throttle drive circuit operation. To date, though, no evidence has been found that such resistive faults have occurred and resulted in a UA incident.
- Although mirroring of critical variables (section 7.5) and ECC is utilized in the RAM to provide protection against bit flips, testing indicated that the system was designed to protect against scenarios where undetected bit flips (e.g. due to memory corruption) led to a request for a large change (exceeding 180°) in the throttle opening request.
- Another important observation made during the HILS testing was that any condition such as a latch-up of the throttle driver circuitry causing wide open throttle or a contaminant that causes the throttle plate to stick, is a fault condition that is detected by the software.

7.10 Summary

Exponent's review of the software system allowed Exponent to reach a number of conclusions.

- Exponent's flow analysis provided an understanding of the interconnection and information flow between the various modules involved with throttle control. Coupled with the line-by-line review performed by Exponent as well as the analysis of the hardware and testing on the vehicle, this analysis helped in understanding the system and identifying failure modes/fault conditions for testing with hardware-in-the-loop simulation. The analysis also ruled out certain identified failure conditions as having the potential of causing UA.
- Fault conditions identified by the flow analysis and the line-by-line source code review, such as bit flips in memory, malfunction of the VSC and/or ECT computer or a malfunction of the modules that calculate the desired

throttle opening angle were simulated using HILS. The simulated fault condition did not identify any software fault conditions that could lead to UA.

- The static analysis performed by Exponent did not identify any run time errors at the language level on the analyzed modules that could cause UA.
- Exponent's review of the fail-safes indicated that the software system was designed to detect both component and system level failures and to prevent the failure of any single component or throttle control related modules from leading to UA.
- A study of the pedal and throttle position algorithms indicated that the vehicle response to pedal failures depended on the nature of the failure, with the vehicle responding with either a dead pedal¹¹³ or a non-linear pedal response (section 4.5) under various fault conditions. However, no fault condition of the pedal/throttle related software design was identified that could explain the reported incidents of unintended acceleration.

Exponent's analysis and testing of the source code did not identify any software fault conditions which can explain the reported incidents of unintended acceleration.

¹¹³ This refers to a condition where the vehicle does not respond to pedal depression (see section 4.8).

8 Other Hardware and System Level Considerations

8.1 Introduction

The preceding chapters have discussed the design, construction and failure modes of the main components comprising the throttle control system on Toyota vehicles equipped with ETCS-i technology. This chapter addresses these issues from a system perspective, including discussions of the network of protection (both in the design and implementation of the ETCS-i system) that guard against failures that could initiate UA. The chapter will discuss the following:

- EMI
- Latch-up
- Software related failures
- Cruise control system
- Resistive Faults

8.2 Electromagnetic Interference (EMI)

EMI can cause the electronics of the vehicle system to transition into an undetermined state or to behave in an unexpected manner. Hazards such as electromagnetic radiation/inductive coupling, noisy power supplies, poor regulation of power supplies etc. all have the potential for interfering with the operation of the vehicle electronics. The ETCS-i system includes various controls at the design, manufacturing and testing stage intended to accommodate EMI to which it may be subjected without causing a system failure. Figure 90 depicts the controls for EMI-related hazards incorporated in the system's hardware and software design, and the vehicle's manufacturing and test processes. The diagram also details the possible vehicle response in the event of an EMI induced failure.

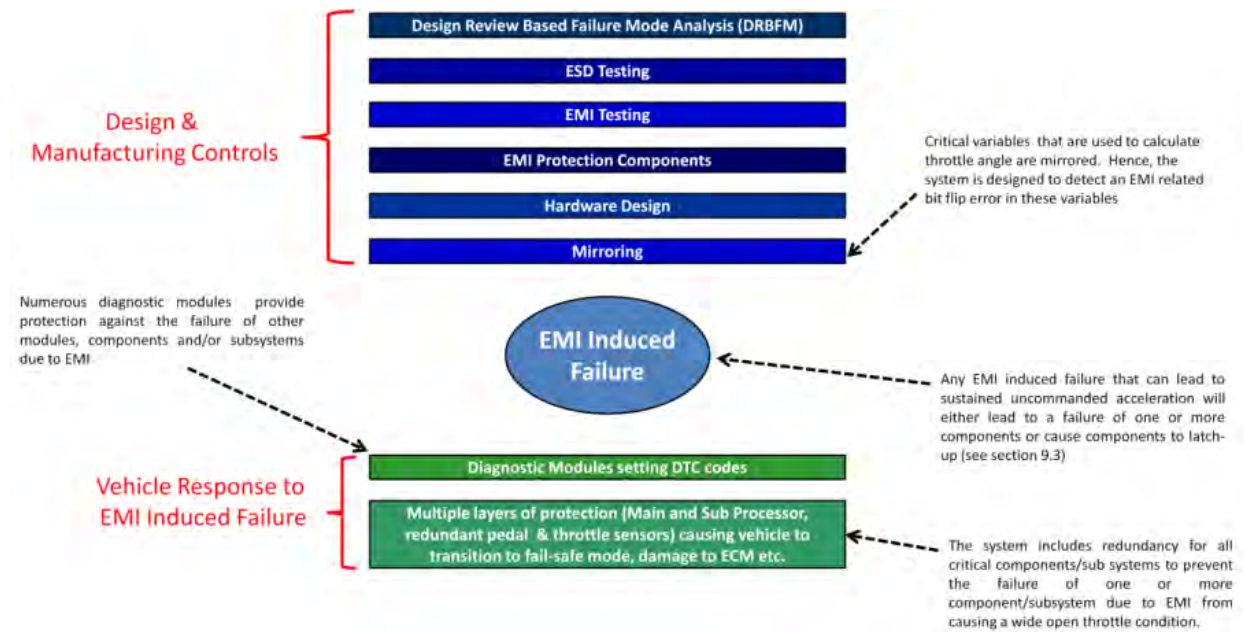


Figure 90. System features that protect against EMI and the system response to EMI induced failures.

Exponent performed extensive EMI testing on multiple Toyota vehicles, including vehicles having each of the technologies used in the accelerator pedal and throttle position sensors. Test methodologies used in these studies included:

1. Anechoic Electromagnetic Chamber dynamometer testing, in which a vehicle running on a dynamometer was subjected to high intensity electromagnetic (EM) radiation.
2. Bulk Current Injection testing, in which electromagnetic noise at discrete frequencies covering a broad spectrum, was coupled directly into the wiring of an operating vehicle.
3. Chatterbox testing, in which multispectral electromagnetic noise consistent with the noise from electrical equipment, such as relay operation, was coupled or injected directly into the wiring of an operating vehicle. This included power supply testing, where the voltage to the ECM of the ETCS-i system, was subjected to large voltage swings.

4. On-board equipment testing, in which signals in the wiring of the ETCS-i system were monitored while on-board equipment (such as power windows, door locks, etc.) was operated.
5. EM Field testing, in which the EM spectrum was measured at locations where strong EM fields are generated, such as antenna farms.
6. Field testing of vehicles, where vehicles were operated in areas with known high EM fields, such as antenna farms, while monitoring the response of the vehicle and induced signals on wiring of the ETCS-i system.
7. ETCS-i system testing in Anechoic Electromagnetic Chambers, where ECM, pedal and throttle body assemblies that had been removed from a vehicle were wired to a vehicle simulator and subjected to high intensity EM radiation. These tests were conducted at higher field intensities than in the vehicle dynamometer testing. Also, components and wiring were exposed to EM fields without any shielding normally provided by the chassis.
8. ETCS-i component testing in Transverse Electromagnetic Cell (TEM cell) chambers, where individual components were subjected to high-intensity EM radiation while their operations were monitored.
9. Magnetic Field testing, where components were subjected to high-intensity time-varying magnetic fields while their operations was monitored.

The testing demonstrated the following:

- Components subjected to EM testing at the highest intensity levels were occasionally observed to fail, but the failures did not result in UA. Component failures triggered the fail-safe modes of operation of the test vehicles.
- The testing confirmed the effectiveness of the hardware and software design, as well as the validation process for the ETCS-i system, against EMI exposure.

- None of the testing identified a root cause that would explain the reported incidents of unintended acceleration.

Details of this EMI testing are provided in a separate Exponent report.

8.3 Latch-up

Latch-up¹¹⁴ pertains to a failure mechanism where a parasitic thyristor (silicon controlled rectifier, or SCR) is inadvertently created within a circuit, causing a current to be continuously conducted through the device once it is triggered or turned on.¹¹⁵ Depending on the circuits involved, the amount of current conducted by this mechanism can be large enough to result in permanent destruction of the device due to electrical overstress. This section of the report describes the phenomenon of latch-up, and considerations for latch-up to occur in Toyota ECMs. The description and test data provided in this section of the report take the 2007 V6 Camry as an example.

8.3.1 Causes of Latch-Up

Latch-up may be caused by a number of triggering factors. To prevent latch-up from occurring, a number of protection schemes are generally applied in hardware designs. Causes of latch-up and protection schemes in Toyota vehicles equipped with ETCS-i technology are:¹¹⁶

- Supply voltages exceeding the absolute maximum ratings
 - A single power supply IC on the ECM provides the supply voltages for all circuits on the ECM. These include two 1.5 Vdc and three 5 Vdc power supplies. Integral voltage regulation in the IC limits the

¹¹⁴ Latch-up, <http://siliconfareast.com/latch-up.htm>

¹¹⁵ “Understanding Latch-Up in Advanced CMOS Logic”, Fairchild Semiconductor Application Note January 1989, Revised April 1999.

¹¹⁶ The 2007 V6 Camry is used as an example for this discussion

voltage variation of the five power supply circuits, preventing the supply voltage from exceeding the absolute maximum ratings.

- The absolute maximum voltage ratings for the ICs used on the ECM exceed the maximum voltage supplied by the power supply IC.
- Input/output pin voltage exceeding either supply rail by more than a diode drop
 - This phenomenon is only applicable to Hall Effect-based sensors which contain active circuits, and not for potentiometric-based sensors which are not subject to the latch-up phenomenon. In Hall Effect-based sensors, the output pins are ratiometrically tied to the input voltage, so if the input voltage increases or decreases, the output signal also changes proportionally. For this reason, the input/output pins on Hall Effect-based sensors will not exceed the supply rail. An output from VPA1 or VTA1 that exceeds rail voltage will set a DTC and cause the engine to operate in fail-safe mode, since such a signal will be out of range.
- Poorly managed power supplies resulting in improper sequencing during start-up
 - All five power supply circuits on the ECM are integrated into a single IC. The control system of the IC ensures proper sequencing of the five power supplies.
- Electrostatic discharge (ESD)
 - Section 6.5 lists the elements for multiple levels of ESD protection on the ECM.
- Electromagnetic radiation
 - Section 6.5 lists the protection elements for multiple levels of EMI protection on the ECM. Latch-up was never observed in any of the

testing, which was conducted at levels that far exceed standards or levels measured in the field.

- Rate of rise of voltage (dV/dt)
 - Section 6.5 lists the protection elements for multiple levels of transient voltage protection on the ECM.
- High thermal stress
 - Heat sinking through the enclosure on ECMs with metallic enclosures limits the thermal stress on the power ICs in the ECM.
 - Data indicates that the rating of ICs and other components is not exceeded under worst case operating conditions. The ECMs are also tested under elevated temperature conditions. As discussed earlier, should an IC on the ECM latch-up, the engine will shut down.
- Inductive transients
 - The ECMs have multiple levels of transient protection as discussed in section 6.5.
- Electrically noisy power supply
 - High frequency decoupling capacitors at the output of the power supply on the ECM regulate the voltages and limit the electrical noise.

8.3.2 Protection against Latch-Up

In addition to the protection circuits discussed in the preceding section, various other protection mechanisms are included in Toyota ECMs that prevent against the occurrence of latch-up. These include:

- Silicon on Insulator (SOI) construction for critical ICs
- Employment of insulating oxide trenches between NMOS and PMOS transistors for critical ICs
- Overall system design
- System low-voltage operation characteristics,

The subsequent sections discuss each of these protection mechanisms.

8.3.2.1 Silicon on Insulator (SOI) Construction

In a silicon-on-insulator (SOI) CMOS technology, the NMOS transistors and PMOS transistors are fabricated on substrates (wells) that are electrically isolated by the silicon dioxide (SiO_2) insulating layer and trenches. Figure 91 is a conceptual cross-sectional view of an inverter circuit in an SOI CMOS process. The parasitic bipolar transistors between the NMOS regions and PMOS regions are suppressed, which fundamentally eliminates the latch-up problem associated with the bulk CMOS process.

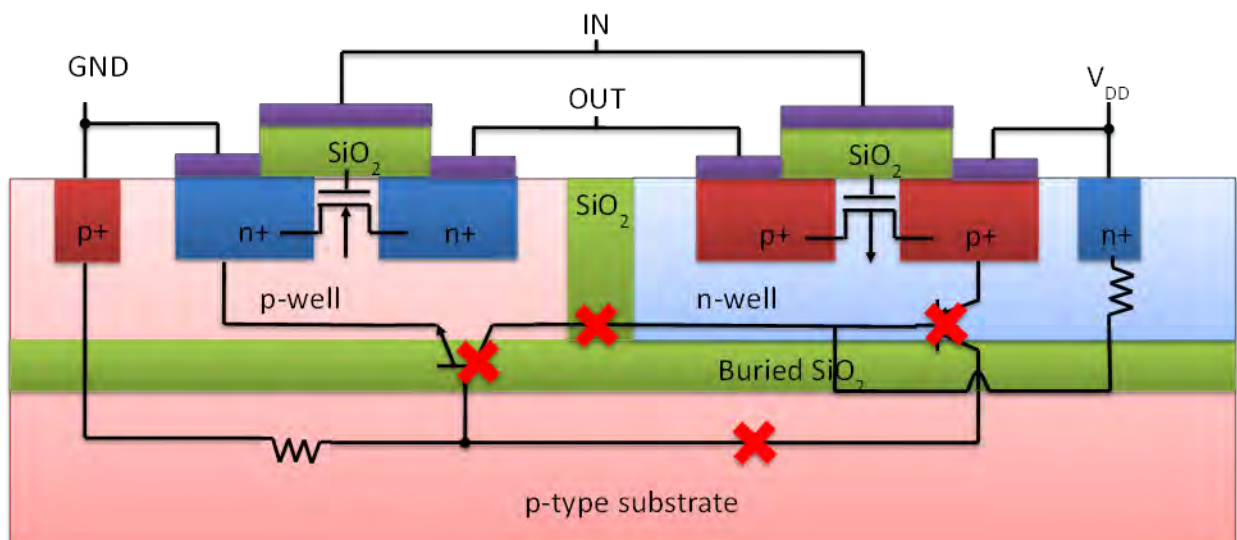


Figure 91. SOI CMOS inverter circuit.

8.3.2.2 SOI Used in ECMs

The ECM in most Toyota vehicles equipped with ETCS-i technology uses a thick oxide, thick epitaxial silicon type of SOI technology for integrated circuits. The use of a relatively thick buried SiO₂ layer and SiO₂ trench isolation enables the integration of multiple types of devices in a single silicon chip, such as:

- CMOS logic transistors
- High voltage power MOSFETs (i.e. Lateral double-diffused MOS transistors or LDMOS-FETs)
- Bipolar transistors.

These SOI BiCMOS/BiCDMOS processes were reported^{117,118,119} to have achieved high temperature (>150°C) and high voltage (>35V) operation, which is relevant for automotive applications. In particular, the use of buried oxide and trench isolation eliminates parasitic transistors in the bulk CMOS technology, thus eliminating some of the high temperature reliability concerns associated with bulk CMOS technology, such as latch-up. Other benefits of SOI technology over bulk CMOS include lower leakage current and lower radiation-induced photocurrents.¹²⁰ The high level integration of both logic and power devices in a single chip also allows for the achievement of more functionality while keeping the cost down. Figure 92 shows a conceptual cross section of devices fabricated in a SOI BiCMOS process from an article published by Toyota.¹²¹

¹¹⁷ M. Hattori, et al “A Powertrain Control SOI BiCMOS LSI for an Automotive Application,” Proceedings 1998 IEEE International SOI Conference, October, 1998

¹¹⁸ M. Hattori, et al “A Very Low On-resistance SOI BiCDMOS LSI for Automotive Actuator Control,” Proceedings 2004 IEEE International SOI Conference, October, 2004

¹¹⁹ H. Himi, et al “Automotive SOI-BCD Technology Using Bonded Wafers,” 17th International Conference on Ion Implantation Technology. AIP Conference Proceedings, Volume 1066, pp. 495-500 (2008)

¹²⁰ C.K. Celler, “Frontiers of Silicon-on-Insulator,” Journal of Applied Physics, Volume 93, Number 9, May, 2003

¹²¹ M. Hattori, et al “A Powertrain Control SOI BiCMOS LSI for an Automotive Application,” Proceedings 1998 IEEE International SOI Conference, October, 1998

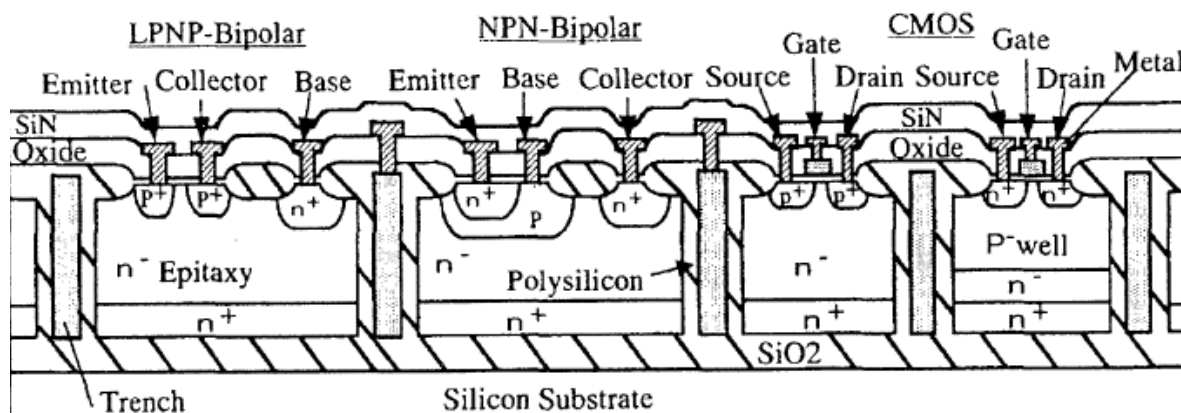


Figure 92. Cross section of bipolar transistors and CMOS transistor fabricated in the SOI BiCMOS process.

According to documents reviewed, all throttle motor driver ICs and power supply ICs used in ECMs of several vehicle models use SOI technology.¹²² In addition, various other input/output interface chips in the ECMs (for example CAN bus interface chips and ignition coil drivers), also typically use SOI technology. In addition to reviewing documents, Exponent also independently collected ECMs used in several Toyota vehicles. Representative samples of this collection were disassembled and examined to determine if the power supply and throttle motor driver ICs used SOI technology. Table 14 provides the list of ECMs examined by Exponent.

Table 14. List of ECMs examined by Exponent

Model	Engine	Year
Tacoma	V6	2007
Tacoma	L4	2009
Camry	V6	2003
Camry	V6	2005
Camry	V6	2007
Camry	V6	2010
Camry	L4	2003
Camry	L4	2005
Camry	L4	2007
Avalon	V6	2006
Sienna	V6	2006

¹²² Except the 2005 – 2008 Corolla. Latch-up conditions and vehicle response for the Corolla vehicles is discussed in Appendix E.

All the power supply and throttle controller ICs in the ECMs examined by Exponent were manufactured using SOI technology. Details of these ICs are discussed in Appendix B.

8.3.3 System Design

Table 15 summarizes the response of the vehicle to a latch-up on one or more ICs that are directly involved with throttle control. The design has numerous fail-safes and safety mechanisms so that a latch-up condition, if it ever did occur, would not lead to UA. Figure 93 provides a high-level summary of the various manufacturing controls and protection features related to latch-up concerns.

Table 15. Mitigations and possible consequences of component latch-up

Component/System	Mitigations & Vehicle Response
Motor Driver Transistor (H-bridge)	Silicon-on-insulator (SOI) construction
	Throttle valve stuck condition causing DTC P2111/P2112
	High current conduction through throttle motor triggers DTC P2103
	Safeguards in the event that fail-safes identified in #2 and #3 above do not operate
	System Guard 2 (Sub Processor) will trigger DTC P2119 if the throttle valve angle differs from the idle and non-linear corrected pedal request by more than 10° (15° if pedal not pressed i.e. vehicle at idle)
	System Guard 1 and/or 3 will trigger DTC P2119 if throttle request and actual throttle angle differ by more than 10°
	Power supply output voltage will drop to approximately 2 V. Both processors will be reset by the Power Supply IC.
Main Processor	If the DTCs don't transition the vehicle to fail-safe mode, the Main processor will cut the fuel and cause the engine to shut-down
	No ignition pulses will be generated. Vehicle engine will stop
	The watchdog timer or direct memory access (DMA) system functionality will cease to function. Vehicle will transition to fail-safe mode
	No communication with the Sub processor. DTC P0607 (Main CPU Failure) will be triggered
	Power Supply IC will reset both the Main processor and the Sub Processor due to a communication error
	Power supply output voltage will drop to approximately 2 V. Both processors will be reset by the Power Supply IC.

Component/System	Mitigations & Vehicle Response
Sub Processor	<p>The Sub processor does not send PWM pulses to drive the throttle motor and open the throttle valve, hence a latch-up of this processor will not send any erroneous commands to the throttle motor driver IC</p> <p>The watchdog timer or direct memory access (DMA) system functionality will cease to function. Vehicle will transition to fail-safe mode</p> <p>The Power Supply IC will reset both the Main processor and the Sub Processor due to a communication error</p> <p>Latch-up may cause the power supply output voltage to drop to approximately 2 V. Both processors will be reset by Power Supply IC if the power supply output voltage drops below approximately 2 V.</p>
Hall Effect Sensor (Pedal & Throttle)	<p>A pedal position sensor failure will be detected and DTC P2123 will be triggered</p> <p>A throttle position sensor failure will be detected and DTC P0123 will be triggered</p> <p>If DTC's don't transition the vehicle to the fail-safe mode, the Main processor will cut the fuel and cause the vehicle's engine to shut-down</p> <p>Power supply output voltage will drop to approximately 2 V. Both processors will be reset by the Power Supply IC.</p>
A/D Converter (Sub Processor)	<p>If a latch-up of the A/D converter occurs, a communication error will result. This will trigger DTC P0607.</p> <p>A pedal position sensor failure will be detected and DTC P2123 will be triggered</p> <p>A throttle position sensor failure will be detected and DTC P0123 will be triggered</p> <p>Throttle valve stuck condition causing DTC P2111/P2112 (valve stuck condition)</p> <p>Power supply output voltage will drop to approximately 2 V. Both processors will be reset by the Power Supply IC.</p> <p>If DTCs don't transition vehicle to fail-safe mode, Main processor will cut the fuel and cause engine to shut-down</p>
Power Supply IC	<p>Silicon-on-insulator (SOI) construction</p> <p>Power supply IC has internal over-current protection circuit. If this IC fails, an over-current condition will either cause the main fuse to open and terminate the current or cause permanent damage to the IC. This damage to the IC will be visible after the latch-up event.</p>

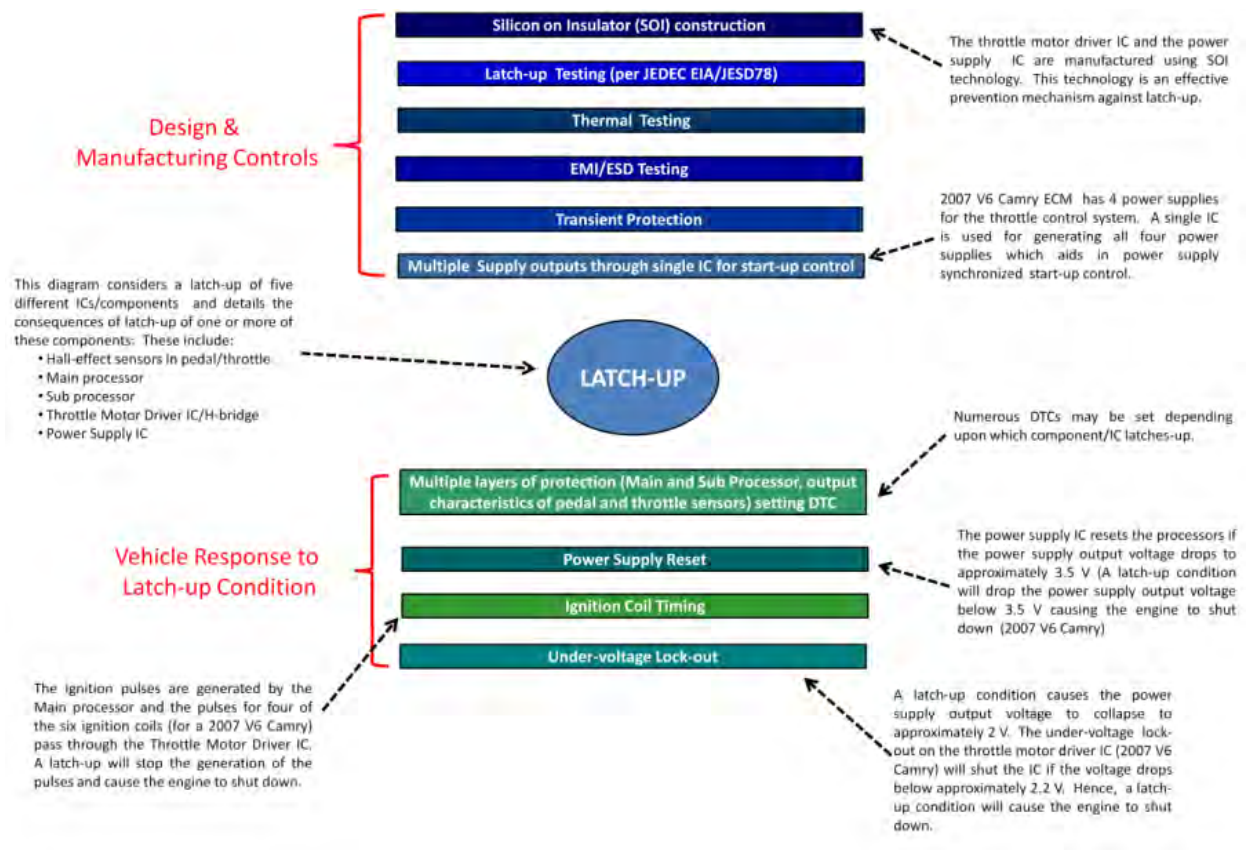


Figure 93. System features that protect against latch-up and the system response to a latch-up condition.

8.4 Software System Guards

In addition to the various modules that monitor individual components, the Main and Sub processor include three system level diagnostic modules that detect a fundamental failure of the system. The three system level modules (also called system guards in the software) are:

- System Guard 1 – Main Processor
- System Guard 2 – Sub Processor
- System Guard 3 – Sub processor.

This section describes how these software level checks monitor and detect failures of a single module or a simultaneous failure of several modules, preventing the vehicle from experiencing UA if these failures occurred in use.

Figure 94 presents a high-level block diagram depicting how the request from the driver (from either the pedal or the cruise control module) is processed and converted to a throttle opening angle. Each of the blocks in the figure below represents several interconnected modules. The three system level checks provide coverage against failure of one or more of these blocks as will be described in this section.

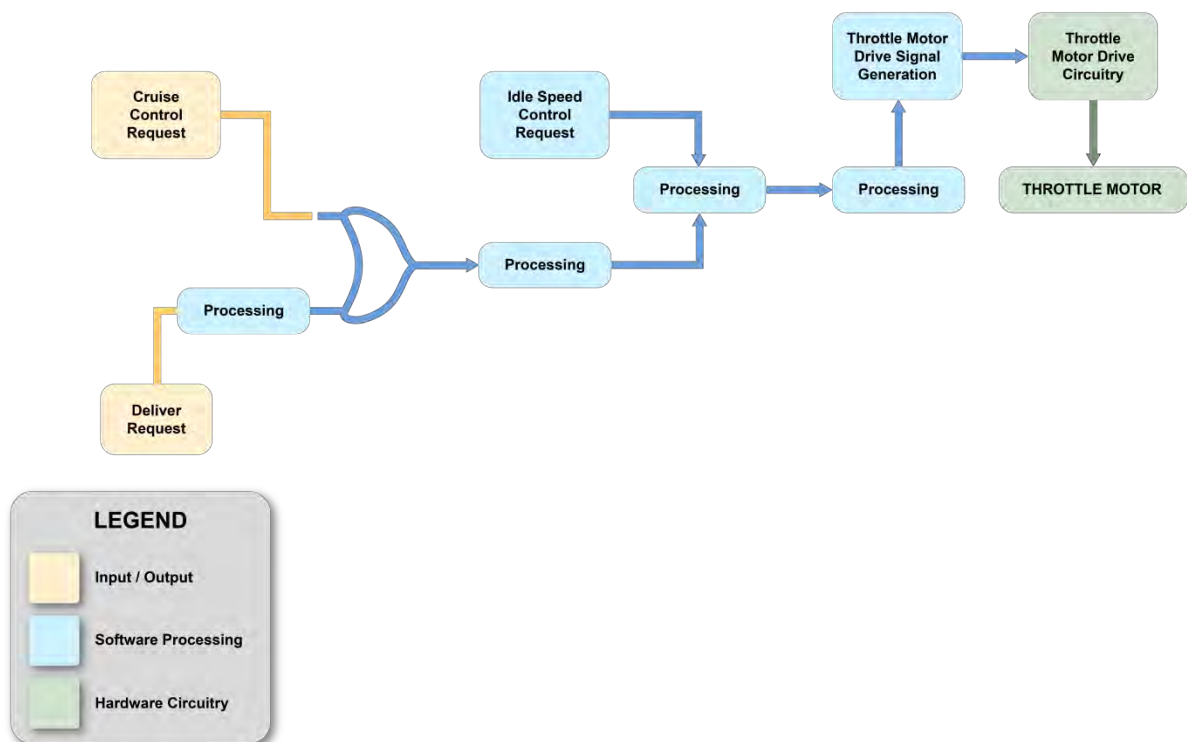


Figure 94. System configuration.

System Guard 1–DTC P2119

The module responsible for triggering this DTC resides and operates in the Main processor. The purpose of this module is to detect an error in the throttle control/drive circuitry. This module compares the throttle instruction value sent to the throttle motor driver IC with the throttle angle detected by the throttle position sensors. A fault detected by this module results in a Class 2 failure. A DTC (P2119) is set under the following conditions (provided a set of other flags are set appropriately):

- (Throttle instruction value – throttle sensor position value) > 0.3 V for [REDACTED]
- (Throttle sensor position value – throttle instruction value) > 0.3 V for [REDACTED].

This module provides coverage against the failure of one or more modules in the Main processor in addition to a failure of the throttle motor driver IC, the throttle motor and/or the throttle position sensors (see Figure 95).

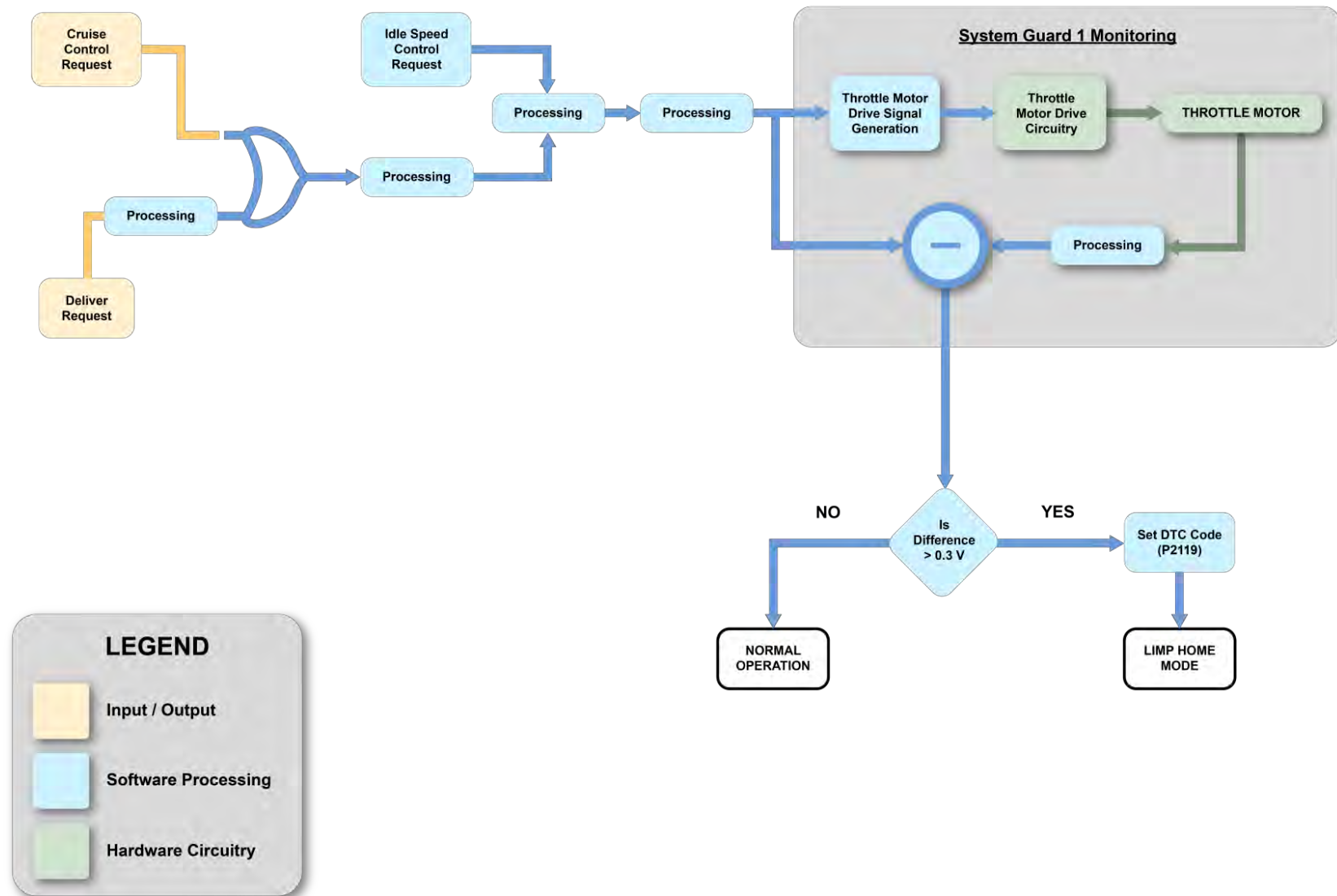


Figure 95. Coverage provided by System Guard 1 (light green block).

System Guard 2–DTC P2119

The module responsible for triggering this DTC resides and operates in the Sub processor. The purpose of this module is to detect an error in the various modules/subsystems that calculate the required throttle opening angle based on the pedal request. This module compares the driver request with the actual throttle opening angle after accounting for the request from the vehicle electrical loads. A fault detected by this module results in a Class 2 failure. A DTC (P2119) is set under the following conditions¹²³:

- When the vehicle is at idle [REDACTED]
[REDACTED]
 - If the following is true for [REDACTED] seconds:

$$(\text{Corrected throttle position value} - \text{throttle opening requirement}) > ([REDACTED]^{\circ} + \text{ISC compensation})^{124}$$
- When the vehicle is not at idle [REDACTED]
[REDACTED]
 - If the following is true for [REDACTED] seconds:

$$(\text{Corrected throttle position value} - \text{driver pedal request}) > ([REDACTED]^{\circ} + \text{ISC compensation})$$

Although the conditions in the bulleted list above seem to include many conditions, the main idea of the two checks is as follows:

- If the vehicle is at idle, the throttle opening angle cannot be more than [REDACTED][°] greater than the throttle opening demanded by the electrical loads through the idle speed control module (ISC module). The throttle opening request from

¹²³ Provided a set of other flags are set appropriately.

¹²⁴ The throttle opening request from the electrical loads is typically 1° to 4° under normal operation. The request from the electrical loads does not exceed [REDACTED][°]. In addition, a secondary check limits the throttle opening request from the electrical loads to 15.5° even under fault conditions.

the electrical loads is typically 1° to 4° under normal vehicle operation. The request from the electrical loads does not exceed \blacksquare° . In addition, a secondary check limits the throttle opening request from the electrical loads to 15.5° even under fault conditions. When the vehicle is being driven (not in cruise control mode), the throttle opening angle cannot be more than \blacksquare° greater than the throttle opening angle demanded by the driver through the pedal (after non-linear correction) and the throttle opening demanded by the electrical loads through the ISC module.

- Assuming that the throttle opening request from the electrical loads through the ISC is 0° , this means that a DTC will be set if the non-linearly corrected pedal request and the throttle opening angle differ by more than \blacksquare° .

This module provides coverage against the failure of multiple modules that calculate the desired throttle opening position in the Main processor in addition to a failure of the throttle motor driver IC, the throttle motor or the throttle position sensors, among other things (Figure 96).

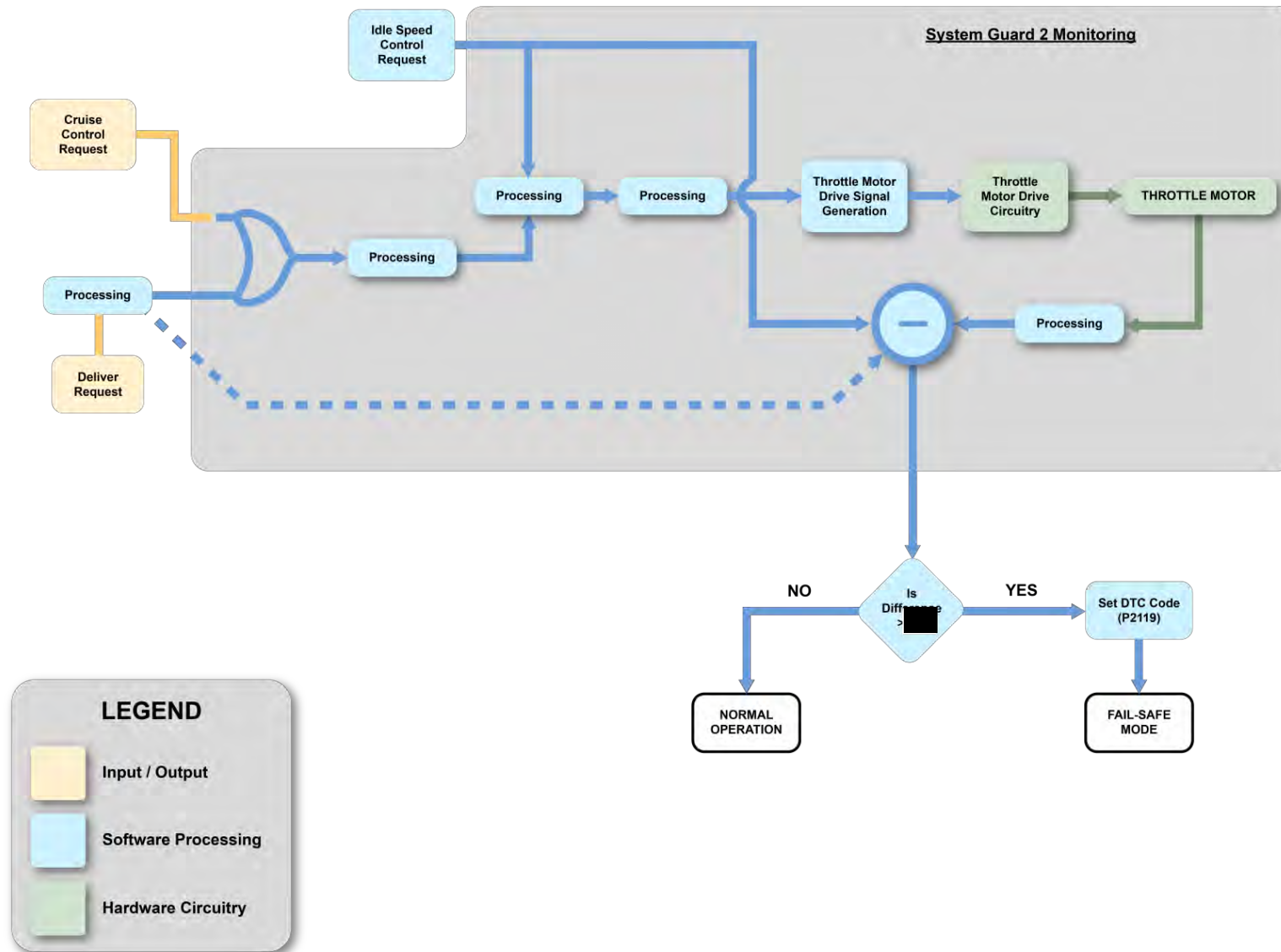


Figure 96. Coverage provided by System Guard 2 (light green box) when the vehicle is being driven.

System Guard 3 – DTC P2119

The module responsible for triggering this DTC resides and operates in the Sub processor. Its functionality is very similar to the functionality of the System Guard 1 module in the Main processor. The purpose of this module is to detect an error in the various modules/subsystems that calculate the pulse width modulated drive signal for the throttle motor that opens the throttle to the desired angle. A fault detected by this module results in a Class 2 failure. This module is run every 10 ms. A DTC (P2119) is set under the following conditions (provided a set of other flags are set appropriately):

- Difference between throttle instruction value and the throttle sensor position value is greater than 1.0 V for 10 seconds.

This module provides coverage against the failure of multiple modules in the Main processor and also the failure of the Main processor to detect this condition.

8.4.1 Summary

The three system level guards provide protection against the failure of multiple components or modules in both the Main processor and the Sub processor. In effect, these modules ensure that:

- A run-away throttle motor condition will be detected even if the Main processor fails.
- In idle mode, the throttle opening angle cannot differ by more than 10° from the opening angle requested by ISC compensation. This means that in the idle mode, the throttle opening angle cannot exceed 10° under the worst case scenario.¹²⁵
- Outside idle mode, the throttle opening angle cannot differ by more than 10° from the non-linearly corrected pedal request angle after accounting for by

¹²⁵ The ETCS-i system is also designed with a fuel cut feature that monitors the engine rpm when the vehicle is at idle (i.e. the accelerator pedal is released). This feature stops the flow of fuel to the engine if the engine speed rises above 2500 rpm with the vehicle at idle.

ISC compensation. In absolute terms this means that the throttle opening angle cannot differ by more than 10° from the non-linearly corrected pedal request under the worst case scenario. However, when the vehicle is being driven, if a fault causes the vehicle to accelerate, the expected driver response will be to release the pedal, which will transition the vehicle to the idle mode (where a DTC is triggered, if the throttle opening angle exceeds the throttle opening request by approximately 10°).

As can be seen by the green boxes in the block diagrams in Figure 95 and Figure 96, the three system guards together provide protection against the failure of most of the modules and/or components/subsystems that control the throttle opening angle. An analysis of the system level flow diagram revealed that the modules not protected by the three system guards have dedicated fail-safes.

8.5 Cruise Control System

Prior to the introduction of electronic throttle control systems in Toyota vehicles, the cruise control functionality was provided by the cruise control ECM and a cruise control actuator on the vehicle. With the introduction of electronic throttle control, the cruise control functionality is now implemented in the ECM. In vehicles equipped with ETCS-i technology, the vehicle speed, the cruise control switch position and the state of the brake switch are monitored by the cruise control-related modules in the ECM (see Figure 97). Depending upon the driver request and the vehicle speed, the cruise control related modules generate and provide a throttle opening request that is used in combination with other sub-system throttle opening requests to generate the overall throttle opening request (see Figure 97).

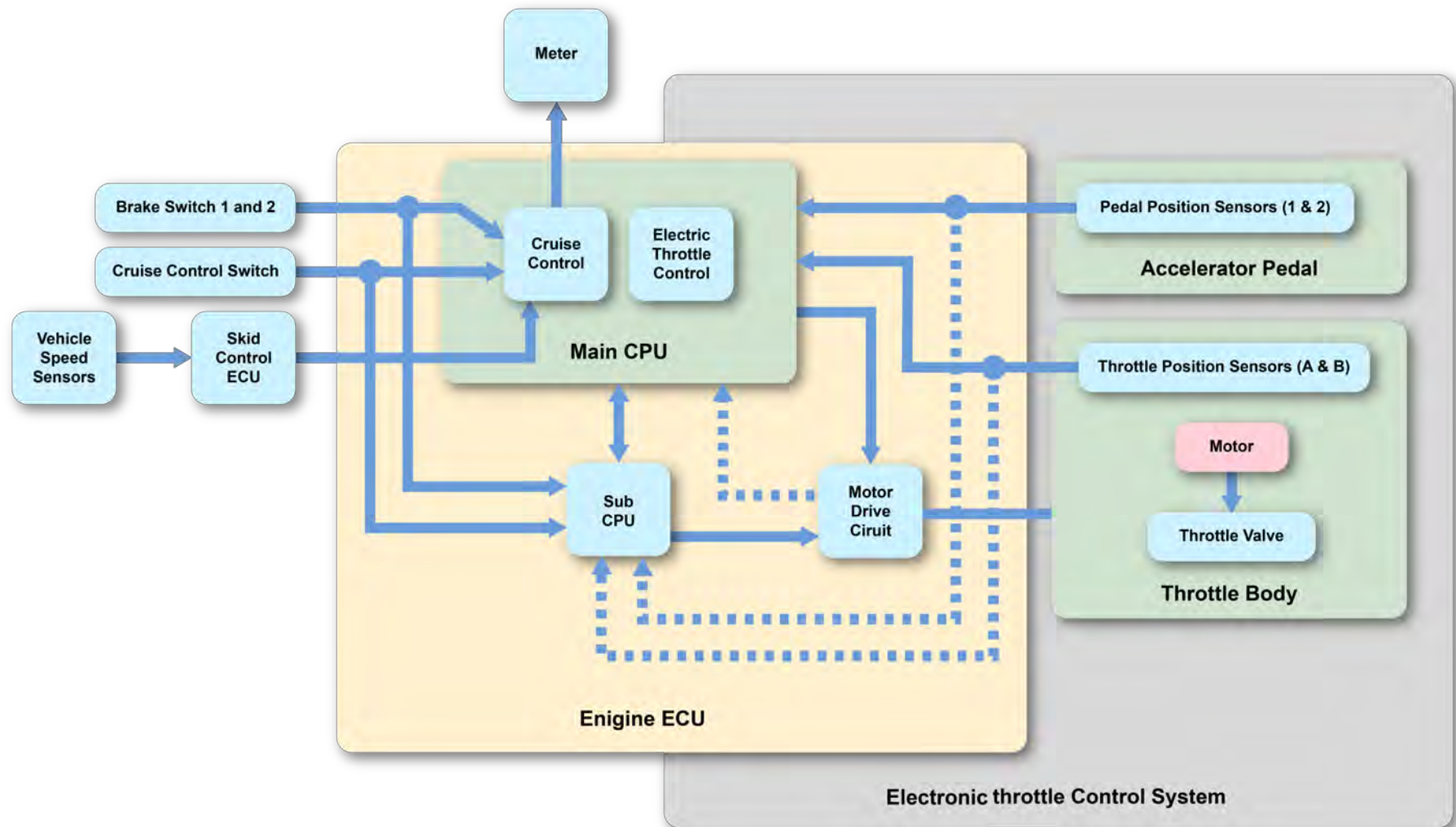


Figure 97. Cruise control system configuration.

8.5.1 Modes of Control

The cruise control system in Toyota vehicles has the following modes of control:

- Constant speed control (Set Control)
 - When the vehicle is set to operate in the constant speed control mode (i.e. the driver turns the cruise control on), the cruise control system stores the vehicle speed and maintains the vehicle at this speed. The throttle valve position is automatically adjusted to maintain the vehicle speed.
 - The cruise control mode cannot be activated for vehicle speeds below 25 miles per hour.
- Increase/decrease speed
 - The cruise control system uses input from the driver provided through the cruise control switch to increase/decrease the vehicle speed in the cruise control mode.
 - If increase speed is selected, the vehicle speed is increased by approximately 1 mile per hour. In addition, if increase speed is selected and held, the vehicle continues to accelerate until the switch is released.
 - Similarly, if decrease speed is selected, the vehicle speed is decreased by approximately 1 mile per hour. If the decrease speed is selected and held, the vehicle speed continues to be reduced until the switch is released.

- Cancel control—Cruise control operation is terminated under any of the following conditions:
 - The brake pedal is depressed
 - Cruise control switch is moved to cancel position
 - Cruise on/off button is pressed
 - When the shift lever is moved from drive to neutral
 - For vehicles with manual transmissions
 - When the ECM receives a neutral position switch signal
 - When the ECM receives a clutch switch signal, which occurs when the clutch is depressed.

Figure 98 is a brief description of the cruise control operation:

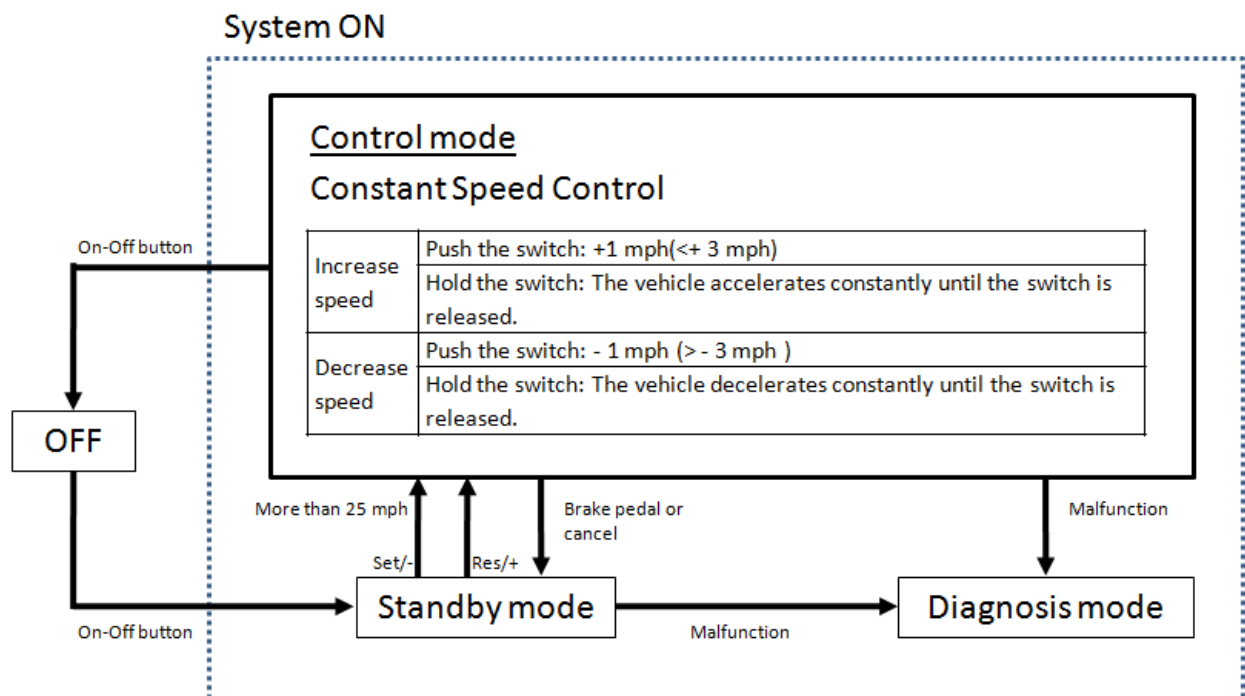


Figure 98. Cruise control operation.

Fail-safes monitor the operation of the cruise control system. In the event that a malfunction occurs, the following actions are performed:

- Cruise control is cancelled
- MIL light turns on
- Cruise indicator light starts blinking
- Information related to the malfunction is stored in memory.

The fail-safes listed in Table 16 are dedicated to detecting cruise control system malfunctions.

Table 16. DTCs related to the cruise control system¹²⁶

DTC	Detection Item	Failure Area
P0500	Vehicle Speed Sensor Malfunction	The vehicle speed signal from the vehicle speed sensor is cut for 0.14 s. or more while cruise control is on. This fail safe detects a failure of the vehicle speed sensor, vehicle speed sensor signal circuit or the ECM.
P0503		Momentary interruption and noise are detected when a rapid change of vehicle speed occurs while cruise control is in operation. This fail safe detects a failure of the vehicle speed sensor, vehicle speed sensor signal circuit or the ECM.
P0571	Brake Switch "A" Circuit Malfunction	When voltage of STP terminal and that of ST1- terminal of ECM are less than 1 V for 0.5 sec. or more. ¹²⁷ This fail-safe detects a failure of the stop light switch, the stop light switch circuit or the ECM.
P0607	Control Module Performance Malfunction	When both of the following conditions are met: STP signals input to the Main processor and the Sub processor are different for 0.15 sec. or more 0.4 sec. have passed after cruise cancel input signal (STP input) is input to the ECM This fail-safe detects a problem with the ECM in cruise control operation.

¹²⁶ These DTCs are for the 2007 V6 Camry.

¹²⁷ The state of the brake pedal is communicated to the ECM using two signals: ST1- (the circuit generating the ST1- signal is only active when the ignition is turned on) and STP. These signals are complementary. The ST1- signal rises from 0 V to the battery voltage and the STP signal drops from the battery voltage to 0 V when the brake pedal is depressed.

8.5.2 Cruise Control and Unintended Acceleration

The cruise control mode is not activated until the vehicle speed exceeds 25 miles per hour. In addition, the cruise control system is deactivated upon brake pedal depression. This means that the cruise control mode can be deactivated by pressing the brake. Testing performed by Exponent using the HILS simulator and a review of the source code related to cruise control operation indicated that even in the event of a malfunction in the cruise control system (i.e. the cruise control system asking for a larger throttle opening request) operation, the driver can safely bring the vehicle to a halt by pressing the brake.

8.6 System Level Protection Features

Figure 99 depicts at system level, the layers of protection related to UA concerns. The layers are grouped into three categories: process/system/design controls, software controls, and hardware controls.

- Process/system/design controls include the conceptual design of the system, quality audits, inspections, testing, failure mode analysis etc.
- Software controls include diagnostic modules, system level fail-safe modules, error correcting codes etc.
- Hardware controls include redundancy in sensors and processors, power supply design, use of SOI technology, etc.

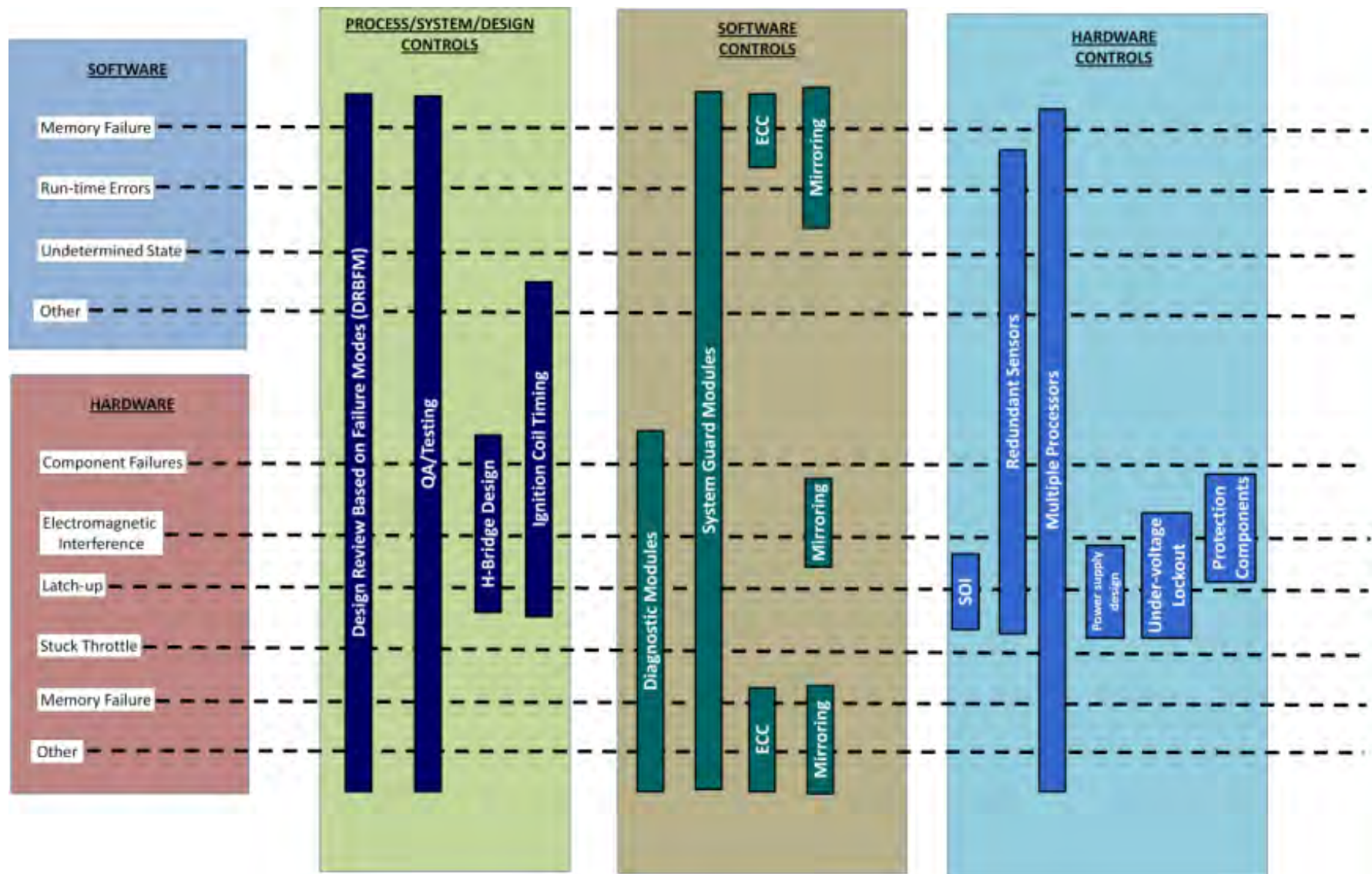


Figure 99. System level protection features.

8.7 Software Failures

Figure 100 shows the levels of protection against software system failures. Hazards such as electromagnetic interference (EMI) causing erroneous signals, logic errors in the code, poor software system design, run-time errors, electrostatic discharge (ESD) etc. all have the potential for causing a failure in the software system. A failure of the software system can transition the system to an undetermined state or cause the vehicle to behave in an unexpected manner. The vehicle manufacturing, design and testing processes (2007 V6 Camry used as an example) act as hazard controls against software failures. In addition, various features included in the software system act as mitigative controls, providing protection to the system in the event of a failure of the software system. These features include multiple fail-safe modules, system level fail-safe modules, and absolute system level checks that limit the deviation in the throttle opening angle from the angle requested by the driver or the cruise control system.

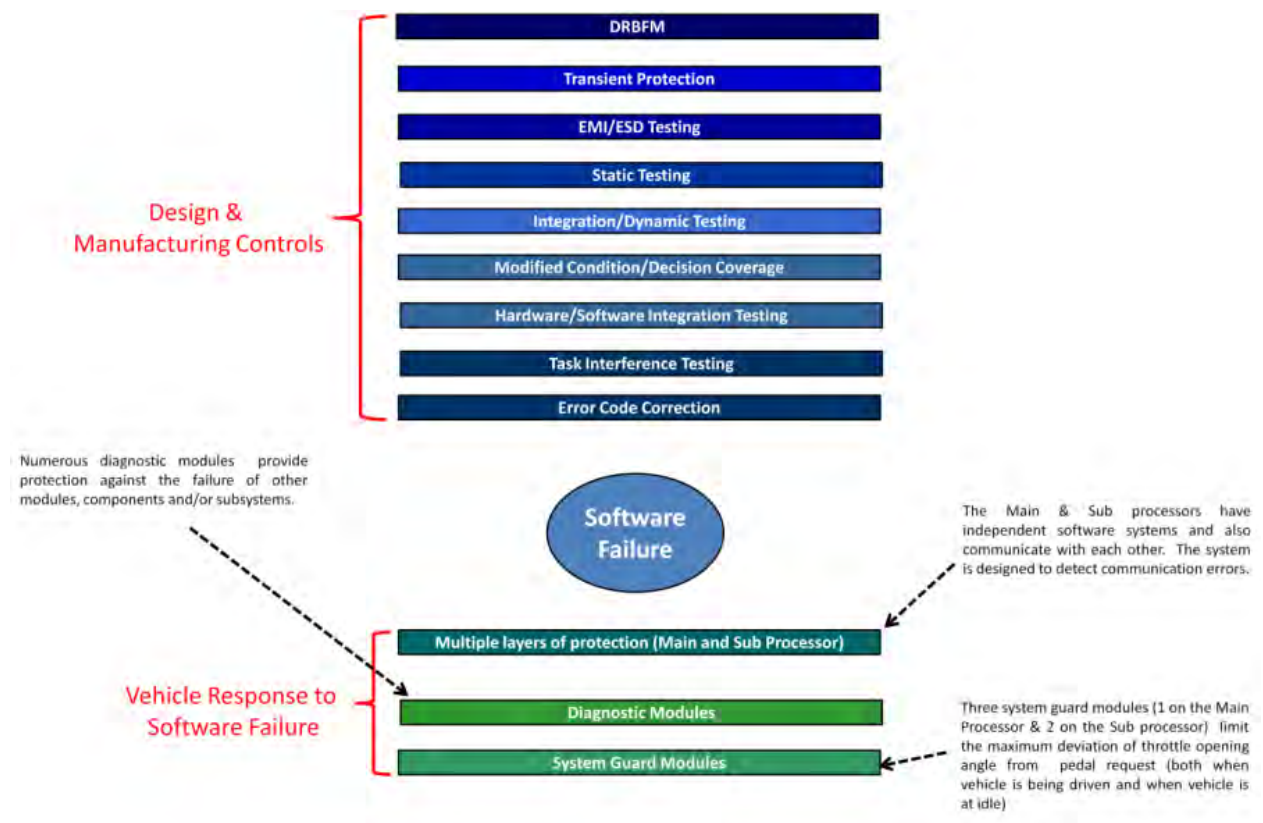


Figure 100. Levels of protection against software system failures.

8.8 Resistive Faults

Resistive faults can potentially arise through a number of mechanisms, including environmentally-driven corrosion, contamination, tin whisker growth and loss of insulation. The vehicle's design, manufacturing, and testing processes include assessments for mitigation or detection of a variety of fault conditions, including ones that might arise from resistive faults. These include:

- In the pedal assembly, two sensors each generate a signal reflecting the pedal position. The sensors are designed not to generate identical signals, but to allow for sufficient differences to facilitate comparison within the software to determine the existence of problems that include resistive faults. Connectors in exposed environments are designed to be waterproof, and include other measures against potentially harmful contamination intrusion, such as gold plating of terminals and individual pin guides.
- The manufacturing processes of the vehicle's hardware components include measures to protect against the development of resistive faults by incorporating environmentally protective features such as potting or conformal coating of electronics, sealing electronics in water-proof enclosures, or placing them in an environment where exposure to moisture and other harsh environmental elements is minimized. With the transition to lead-free soldering, manufacturing processes were designed to address the potential for tin whisker growth. These processes include material selection (such as the use of Ni-Pd-Au platings on the closely-spaced IC pins), ensuring adequate spacing between contacts, coatings on the electronics, and testing to identify tin-whisker potential.
- Toyota Quality assurance and control processes require the testing of hardware and software components under specific environmental and electrical conditions. Results of such testing are fed back into the design process to ensure mitigation actions are taken to address the cause or consequences of faults discovered during this process.

- The ECM is programmed to look for, and react to, problems that might arise with sensor electronics. In Toyota vehicles, problems with the electronic throttle control system will illuminate the malfunction indicator light and transition the vehicle to a fail-safe mode of operation.
- The different levels of protection against potential negative effects of resistive faults, which encompass design, manufacturing and testing processes, along with safety mechanisms in hardware and software are summarized in Figure 101. Exponent has not identified a realistic set of conditions that would result in UA in a manner consistent with unintended acceleration complaints, without deliberate manipulation and re-engineering of the vehicle's electronics (see section 4.7 for further details)

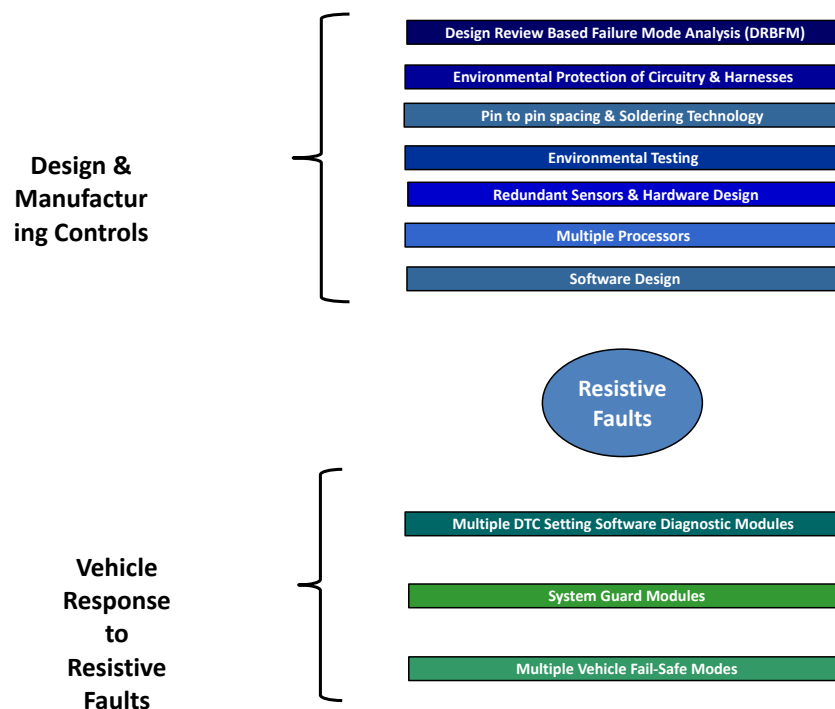


Figure 101. Levels of protection against resistive faults.

9 Parts Collected for Study

9.1 Introduction

As part of its investigation, Exponent collected new and used parts for study and testing. In addition, Exponent inspected six vehicles that were alleged to have experienced a unintended acceleration event (three of these vehicles were purchased by Exponent for more detailed testing). This chapter details the results of Exponent's inspections.

9.2 Inspection of Field Components

More than 520 new and used components were acquired for inspection by Exponent, with over 420 parts from various models and model years of Toyota and Lexus vehicles, and over 100 parts from various model and model years of other vehicle makes. The parts acquired for inspection included accelerator pedals and pedal position sensors, throttle bodies and throttle position sensors, electronic control modules, wiring harnesses, cruise control units, electrical connectors, and floor mats. A summary of the acquired components by component type and vehicle model and model year are provided in Appendix D. In addition to the acquired components, 42 Toyota and non-Toyota vehicles were acquired for inspection and testing.

9.2.1 Component Inspections and Resistive Contaminations

One of the objectives of Exponent's component inspections was to identify possible contamination at the electrical connectors of the position sensors. Used components were acquired from vehicle salvage yards for inspection. Environmental exposure while in the salvage yard could be significant (Figure 102). Electrical connectors were visually inspected for signs of corrosion or dendrite growth between the connector pins, as well as for signs of moisture or contaminant intrusion inside the connectors and the sensors. Current-limited electrical insulation testing was performed at elevated voltages to determine the levels of insulation resistance between the sensor signal wires. If conductive contamination had bridged

connector pins, the insulation resistance would have been significantly lowered due to the conductivity of the contaminants. Figure 103 shows a sample accelerator pedal connector and connector circuit diagram as well as the insulation resistance measurement method. Inspection and electrical testing of used parts acquired from the vehicles did not identify any electrical connections from external contamination.



Figure 102. Used vehicle parts were acquired for resistive contamination testing.

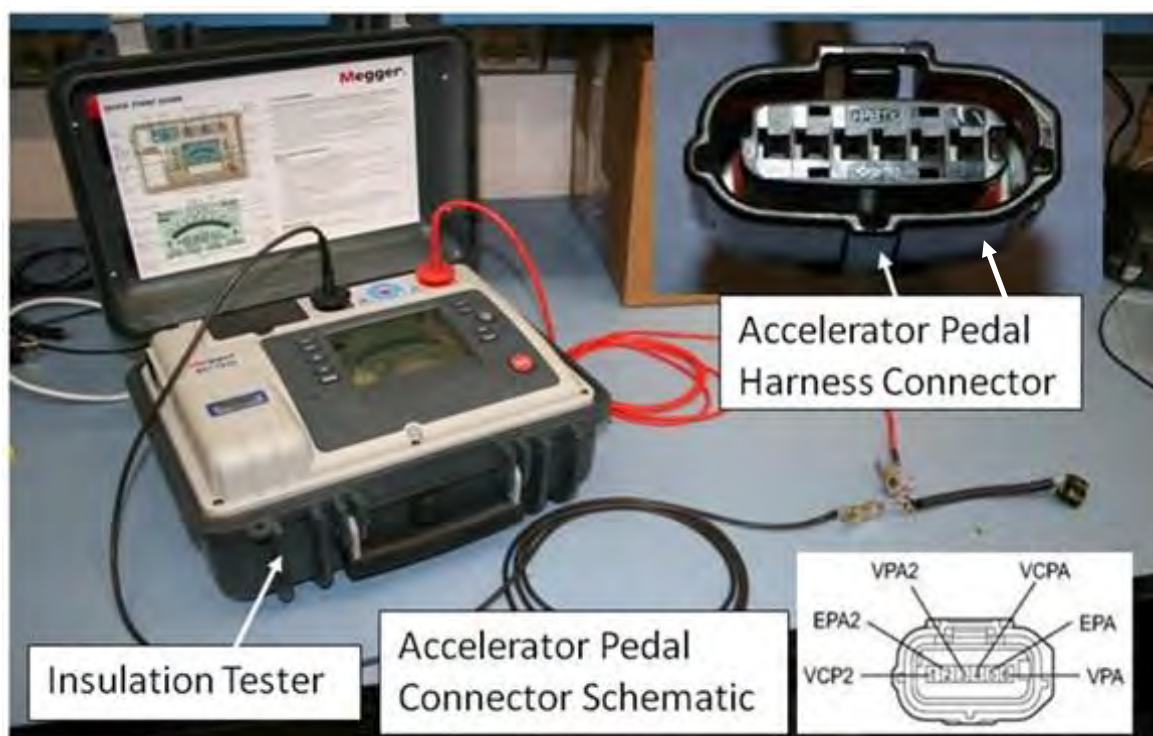


Figure 103. Insulation test method to measure surface resistances due to contaminants.

In addition to the connectors at the accelerator pedal, throttle body and electronic control module, some vehicles such as the Toyota Tacoma have an intermediate connector between the accelerator pedal position sensor and the Electronic Control Module (ECM). The possibility of resistive connections between the signal wires of the accelerator pedal due to contaminants in the Toyota Tacoma was investigated. Six wiring harnesses from used Tacomas were acquired. The condition of the pedal connectors and the intermediate connectors were visually inspected and photographed (See Figure 104). Insulation resistance measurements were also performed. No contamination or parasitic resistances were found at the connectors.

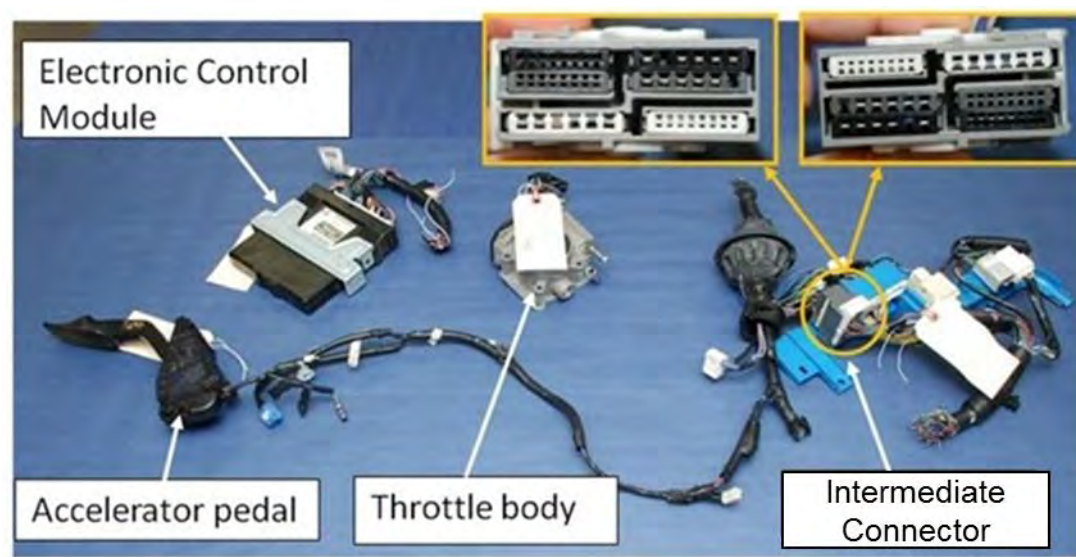


Figure 104 Wiring harness of Toyota Tacoma including the pedal, ECM and the intermediate connector.

9.2.2 Component Inspections and Tin Whisker Investigations

More than 50 parts from Toyota and non-Toyota vehicles were inspected for tin whiskers. Inspected parts included accelerator pedals and throttle body sensors as well as different components from inside the electronic control module. Of the parts inspected for tin whiskers, more than 40 were from different models of Toyota and Lexus vehicles. The remaining parts were from competitor vehicles such as Honda, BMW, Chevrolet and Ford. A list of parts inspected for tin whiskers is shown in Table 17.

Table 17 List of parts used by Exponent for inspections regarding the matter of tin whiskers

Make	Model	Model Year	Component	Make	Model	Model Year	Component
Honda	Accord	2008	ECM	Toyota	Camry	2010	Pedal Sensor
Toyota	Avalon	2006	Pedal Sensor	Toyota	Camry Hybrid	2008	ECM
BMW	325i	2002	ECM	Toyota	Camry Hybrid	2008	Pedal Sensor
Toyota	Camry	2002	ECM	Toyota	Camry Solara	2007	Pedal Sensor
Toyota	Camry	2002	ECM	Toyota	Camry Solara	2008	ECM
Toyota	Camry	2002	Pedal Sensor	Toyota	Camry Solara	2008	Pedal Sensor
Toyota	Camry	2002	Pedal Sensor	Chevrolet	Cobalt	2010	ECM

Make	Model	Model Year	Component	Make	Model	Model Year	Component
Toyota	Camry	2002	Pedal Sensor	Toyota	Corolla	2007	Pedal Sensor
Toyota	Camry	2003	ECM	Toyota	Corolla	2008	Pedal Sensor
Toyota	Camry	2003	ECM	Toyota	Corolla	2008	Pedal Sensor
Toyota	Camry	2003	Pedal Sensor	Toyota	Corolla	2009	ECM
Toyota	Camry	2003	Throttle Sensor	Toyota	Corolla	2009	Pedal Sensor
Toyota	Camry	2004	Pedal Sensor	Ford	Fusion	2009	ECM
Toyota	Camry	2005	Pedal Sensor	Ford	Fusion	2007-2009	ECM
Toyota	Camry	2005	Pedal Sensor	Toyota	Lexus SC430	2002	Pedal Sensor
Toyota	Camry	2005	Pedal Sensor	Toyota	Lexus SC430	2003	Pedal Sensor
Toyota	Camry	2007	ECM	Toyota	Matrix	2009	Pedal Sensor
Toyota	Camry	2007	Pedal Sensor	Toyota	Scion	2008	Throttle Sensor
Toyota	Camry	2009	ECM	Chevrolet	Silverado	2010	ECM
Toyota	Camry	2009	Pedal Sensor	Toyota	Solara	2006	ECM
Toyota	Camry	2009	Pedal Sensor	Toyota	Solara	2006	Throttle Sensor
Toyota	Camry	2009	Pedal Sensor	Toyota	Tacoma	2009	ECM
Toyota	Camry	2009	Pedal Sensor	Toyota	Landcruiser	2006	Pedal Sensor
Toyota	Camry	2009	Pedal Sensor	Toyota	Tundra	2010	ECM
Toyota	Camry	2009	Pedal Sensor	Toyota	Yaris	2008	ECM
Toyota	Camry	2010	ECM	Toyota	Yaris	2008	Pedal Sensor

In addition to the inspected parts, two vehicles were inspected for the possibility of tin whisker growth in the accelerator pedal sensor assembly. The inspected vehicles were a 2002 Toyota Camry (4T1BE32KX2U593139) and a 2005 Toyota Camry (4T1BE32K85U403343). Both of these vehicles had been brought to Toyota dealerships for diagnosis and repair related to hesitation in the throttle response. The preliminary diagnosis made by the Toyota technicians indicated that a resistive fault was present between VPA1 and VPA2. In both vehicles, Exponent inspections determined that a resistive connection was present inside the potentiometer-type accelerator pedal position sensors. In both vehicles, this fault was detected by the ECM and indicated by a stored DTC and Malfunction Indicator Lamp.

9.2.3 Component Inspections and Continuity Measurements

The potential for the formation of a resistive contact between mating connector leads was investigated. Connectors for accelerator pedal sensor, throttle body sensor, ECM connectors and other ETCS-i-related connectors harvested from used vehicles were electrically tested and visually inspected for corrosion or contamination, which could cause resistive paths in a sensor connector. This phenomenon is known as a series resistive fault.

Continuity measurements were performed using a digital multimeter to measure resistance of the sensor signal wires from the pedal to the ECM. Continuity testing was performed, particularly for the Toyota Tacoma, to inspect the possibility of resistive paths at the intermediate connectors. Electrical testing did not identify any resistive connections. Visual inspections of the connectors showed no sign of corrosion or contaminants that are usually the cause of series resistive faults.

9.3 Incident Vehicle Inspections

Exponent inspected six vehicles in which a driver reported an unintended acceleration event. Exponent purchased three of these vehicles in order to perform more detailed testing. During the inspections, to the extent permitted, Exponent performed a series of tests that included:

- Electrical measurements on the accelerator pedal, throttle body, and wiring harnesses to check for resistive faults, open circuits or short circuits
- The ECM was queried for DTCs
- The event data recorder (EDR), if present, was queried to identify conditions prior to any event, if a triggering event occurred
- Driving tests
- Functional measurements on accelerator pedal and throttle valve

- Visual inspection of the vehicle, including components of the ETCS-i system and wiring
- Supplemental testing consistent with descriptions of the reported unintended acceleration incident.

These tests were performed to find evidence of possible causes for reported unintended acceleration incidents.

9.3.1 Vehicles Inspected

Data on the vehicles inspected are provided in Table 18.

Table 18. List of inspected vehicles with reported unintended acceleration incidents

Make	Model	Year	VIN	Mileage at inspection	Exponent Purchase
Toyota	Corolla	2009	1NXBU40E79Z118435	8,974	X
Toyota	Tacoma	2009	5TEUU42N99Z658130	13,354	X
Toyota	Tundra	2007	5TBBV54187S486597	34,353	X
Toyota	Camry	2004	4T1BE32K04U299493	49,708	
Lexus	GX470	2003	JTJBT20X830013556	35,716	
Toyota	RAV4	2004	JTEGD20V940023093	27,156	

The ETCS-i technology and EDR equipped on each of these vehicles is shown in Table 19.

Table 19. Technology used on inspected vehicles

Vehicle	Pedal Position Sensor Manufacturer/ Technology	Throttle Position Sensor Manufacturer/ Technology	ECM Manufacturer/ Location	Summary of data stored on EDR
2009 Corolla	CTS/ Hall effect	Denso/ Hall effect	Delphi/ Engine Compartment	No event data stored.
2009 Tacoma	Denso/ Hall effect	Denso/ Hall effect	Denso/ Behind glove box	No event data stored.
2007 Tundra	CTS/ Hall effect	Denso/ Hall effect	Denso/ Engine Compartment	Data from a non-deployment rollover event stored. Maximum roll angle was 7 degrees; no pre-crash data was stored.
2004 Camry	Aisan/ potentiometer	Denso/ Hall effect	Denso/ Behind glove box	No EDR Download Attempted
2003 GX470	Denso/ Hall effect	Denso/ Hall effect	Denso/ Behind glove box	No EDR Download Attempted
2004 RAV4	Aisan/ potentiometer	Denso/ Hall effect	Denso/ Behind glove box	3 events stored, no pre-crash data available for this vehicle.

9.3.2 Findings

The following was observed during the vehicle inspection/testing:

- No shorts or resistive faults were found, and sensor voltage measurements were within specifications for all inspected vehicles. In addition, sensor connectors were removed and inspected (to the extent possible) to look for signs of contamination. No signs of contamination were found inside the connectors on any of the vehicles.
- For all vehicles except the RAV4 (which was damaged in a crash), test drives were performed to find evidence of possible causes. Except for the 2004 Camry (discussed later), the test drives did not identify any anomalous performance.
- The 2009 Corolla was eligible for recall for both the CTS accelerator pedal and for potential floor mat interference. At the time of the inspection, the accelerator pedal had not had the recall work performed. A carpeted floor

mat was installed in the vehicle, and the hooks were properly positioned at the time of the inspection.

- The 2007 Tundra was eligible for recall for both the CTS accelerator pedal and for potential floor mat interference. At the time of the inspection, the accelerator pedal had not had the recall work performed. An all-weather floor mat was positioned on the carpeting at the time of the inspection.
- The throttle body on the 2004 Camry was found to be mechanically sticking, and the TechStream download revealed DTC P2112 (*Throttle Actuator Control System – Stuck Closed*). Visual inspection of the throttle body showed evidence of corrosion, and manual manipulation of the throttle revealed mechanical binding. The vehicle's corroded and sticking throttle body was similar to that described in Toyota Technical Service Bulletin T-SB-0187-09.
 - As part of the inspection of the 2004 Camry, the throttle was intentionally stuck open at varying angles before starting the engine. In all cases accelerator input consistently resulted in setting a DTC and stalling of the engine. The vehicle moved without pedal application, however; in this condition, the vehicle attained a maximum speed of approximately 25 mph on a flat level surface. The vehicle speed could easily be controlled with brake pedal application, and any accelerator pedal input caused the engine to stall. When testing the vehicle, the stuck throttle was consistently detected, resulting in a DTC being set and the vehicle transitioning to the limp-home mode.
 - The behavior in the 2004 Camry was consistent with the vehicle owner's report of the vehicle repeatedly stalling. When the owner experienced the event he reported as unintended acceleration, he had restarted the vehicle and was likely driving without having applied the

accelerator pedal, in a similar manner that Exponent was able to drive the car up to approximately 25mph.

- The behavior observed in the 2004 Camry does not result in a dangerous UA condition and is easily identifiable during a vehicle inspection.

The inspection and testing performed on vehicles alleged to have experienced unintended acceleration did not identify a mechanical or electrical cause for the reported incidents.

10 Connectors and Wiring

10.1 Introduction

This chapter will address the types of connectors used and design features of connectors used on accelerator pedals, throttle assemblies, and ECMs. In addition, potential failure modes associated with connectors and wiring harnesses will be addressed. The following items will be addressed as part of this discussion:

- Types of connectors and their construction
- Wiring insulation and wiring harnesses.

10.2 ECM Connectors

Connectors on the ECM are used to transmit or receive power, communication signals and sensor signals. ECM connectors are of two general types depending upon the location of the ECM in the vehicle.

- Non-waterproof connectors
- Waterproof connectors.

10.2.1 Non-waterproof Connectors

Toyota vehicles equipped with ETCS-i that have ECMs located in the passenger compartment use non-waterproof connectors on the ECM. These ECMs are generally located behind interior trim, such as adjacent to the glove box under the dashboard (see Figure 105). This location is protected from direct contact with liquids or sprays. The non-waterproof connectors on the ECM have the following features:

- The connector pins are coated with either tin or gold to provide resistance to corrosion, reduction of wear of the contact surfaces, and reliable operation throughout their expected life.
 - The signal pins such as the throttle pins and the pedal position pins are gold-plated and corrosion resistant preventing resistive contacts from forming.
 - The power pins, including those that supply electric power to the throttle motor, are tin plated.
- The wires are individually insulated, bundled, protected and routed away from exposure to the cabin.
- The connectors have locking mechanisms to prevent them from disengaging in service. Each connector has a different profile, so that the connectors cannot be inadvertently interchanged.
- These connectors are not normally exposed to liquid immersion. However, should liquid intrusion occur, electrical connection between contacts would be hampered by the individual pin guides. Should contamination cause a parasitic resistive electrical connection to form, evidence of such intrusion and the resulting parasitic resistive electrical connection(s) would remain. Turning the car ignition off and then on would not cause such evidence to disappear. Liquid intrusion that causes a resistive short would leave a visible “signature.”



Figure 105. View of ECM installation in a 2003 V6 Camry. Interior trim and the glove box have been removed so the ECM can be seen.

Figure 106 shows the male, non-waterproof ECM connector for a 2002 Camry. The cover has been removed from the ECM. Figure 107 shows the female non-waterproof ECM connector of the same vehicle.



Figure 106. Male ECM connector for a 2002 V6 Camry. The ECM cover has been removed. Yellow arrow points to the gold-plated pins used for the throttle signals. Blue arrow shows the gold-plated pins used for the accelerator pedal position sensor signals. Green arrows show the tin-plated pins used for the power signals sent to the throttle motor.

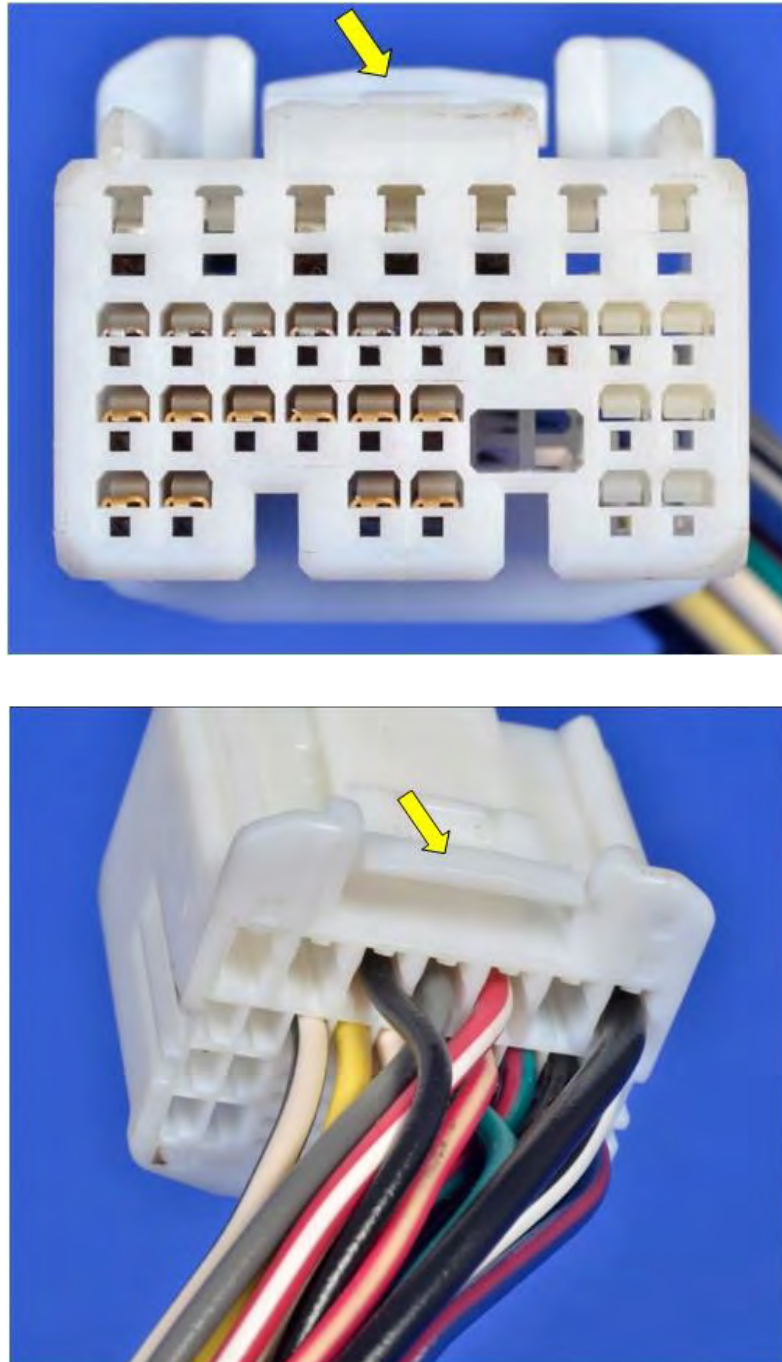


Figure 107. Female, non-waterproof ECM connector for a 2002 V6 Camry. The wires are individually insulated, bundled, protected and routed away from penetrations. Yellow arrows show the locking mechanism.

10.2.2 Waterproof Connectors

ECMs located in the engine compartment use waterproof connectors. These ECMs may be exposed to automotive fluids, or contaminants in the engine compartment. The male portion of the connector (Figure 108) is attached to the ECM circuit board and the female portion is attached to the connecting wire harness (red and blue arrows in Figure 110). Polymeric grommets in the female portion of the connectors form the waterproof seal between the connector halves.

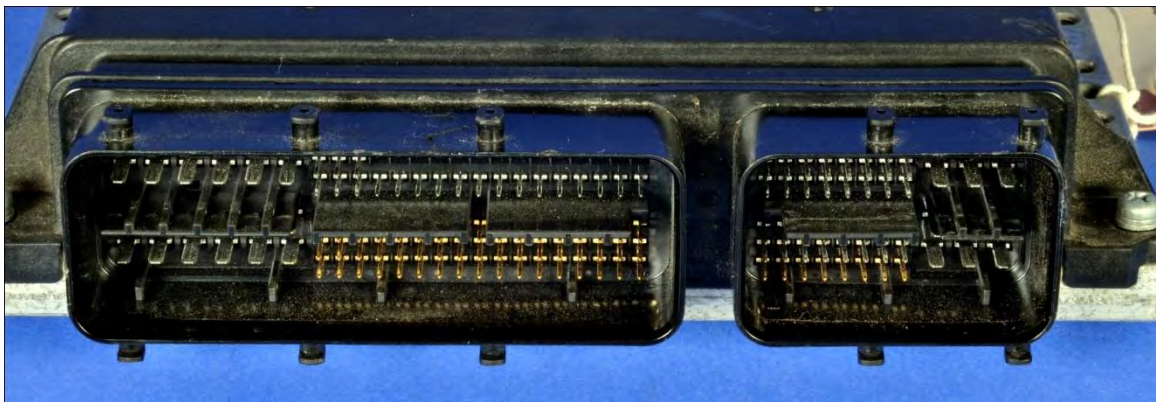


Figure 108. Male portion of the ECM connector.

The ECM connector pins include power pins and signal pins. The male and female contact pins have a contact finish to provide corrosion protection for the base metal. The pins are coated with either tin or gold to provide resistance to corrosion, reduction of wear of the contact surfaces, and reliable operation. The waterproof connectors on the ECM have the following features:

- The connectors contain seals that are designed to prevent liquid intrusion into the connector contact region. In addition, both the mating connector bodies and the individual conductors are sealed against liquid intrusion.
- The connectors have locking mechanisms and are mechanically locked to components to maintain a reliable connection. The two halves of the ECM connector cannot be separated without the disengagement of an interlocking clasp.

The yellow arrows in Figure 109 and Figure 110 show a sample lock configuration. Other locking mechanisms have also been employed. When separated, the connector's two halves reveal features of the connector, which include a protective shell, polymer gaskets, insulated wires, and recessed pins.

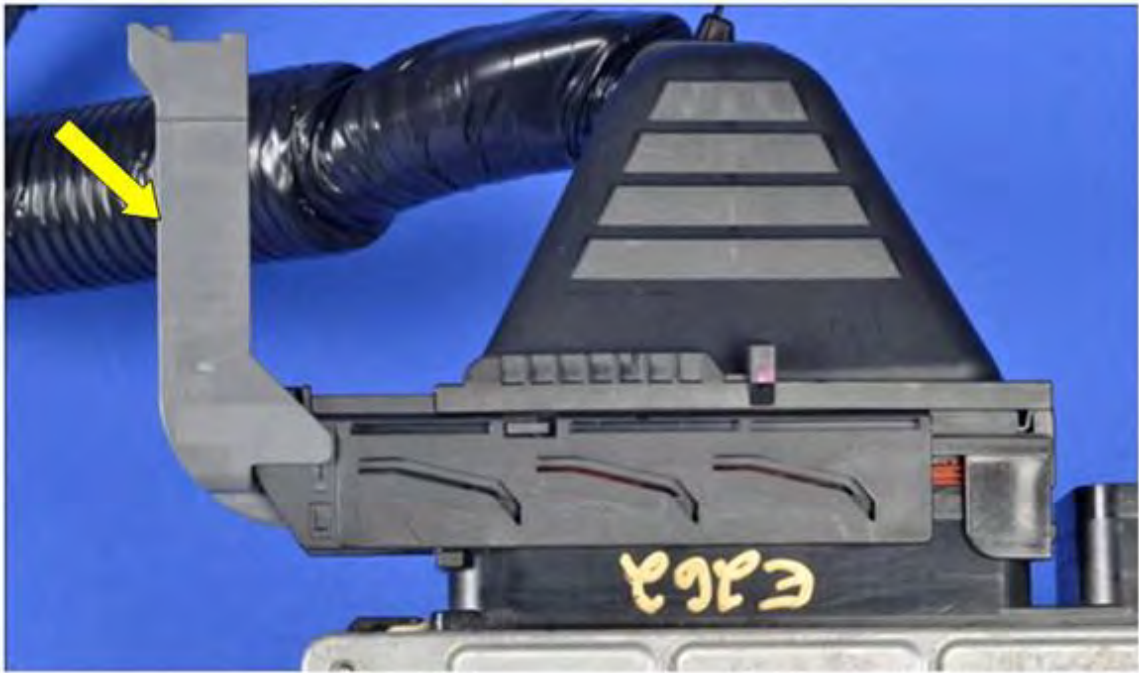


Figure 109. ECM connector. Arrows show the gray connector locking mechanism.



Figure 110. ECM connector in locked position and portion of wiring harness. Yellow arrow shows locking gray connector in locked position.

The female portion of the connector is designed with the following features:

- A plastic shell surrounding the housing of the male portion of the connector to prevent direct moisture contact.
- A rubber gasket that surrounds the rim of the female portion, making the connector waterproof (Figure 111)
- Each pin fits into its own insulated slot to electrically isolate the individual pins from each other (Figure 112).
- Recessed pin sockets that reduce the possibility of electrical interconnection between adjacent pins.
- A plastic divider that extends into the connector further reducing the possibility of electrical interconnections between adjacent pins.
- Insulation on each connector lead

- The waterproof ECM connectors have a polymeric grommet which provides protection to each connector lead to make it waterproof and to provide additional electrical insulation (Figure 112).
- The wires are spaced to prevent adjacent wire contact.

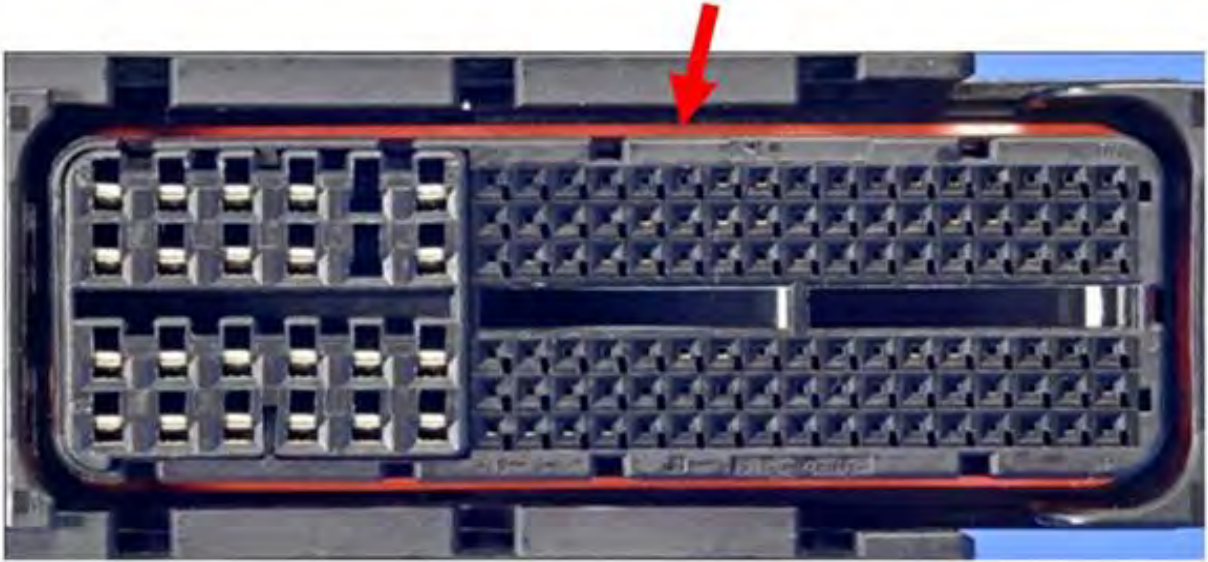


Figure 111. ECM female connector assembly for the large connector. A rubber gasket (red arrow) on the rim of the connector housing is used to make the connection waterproof.

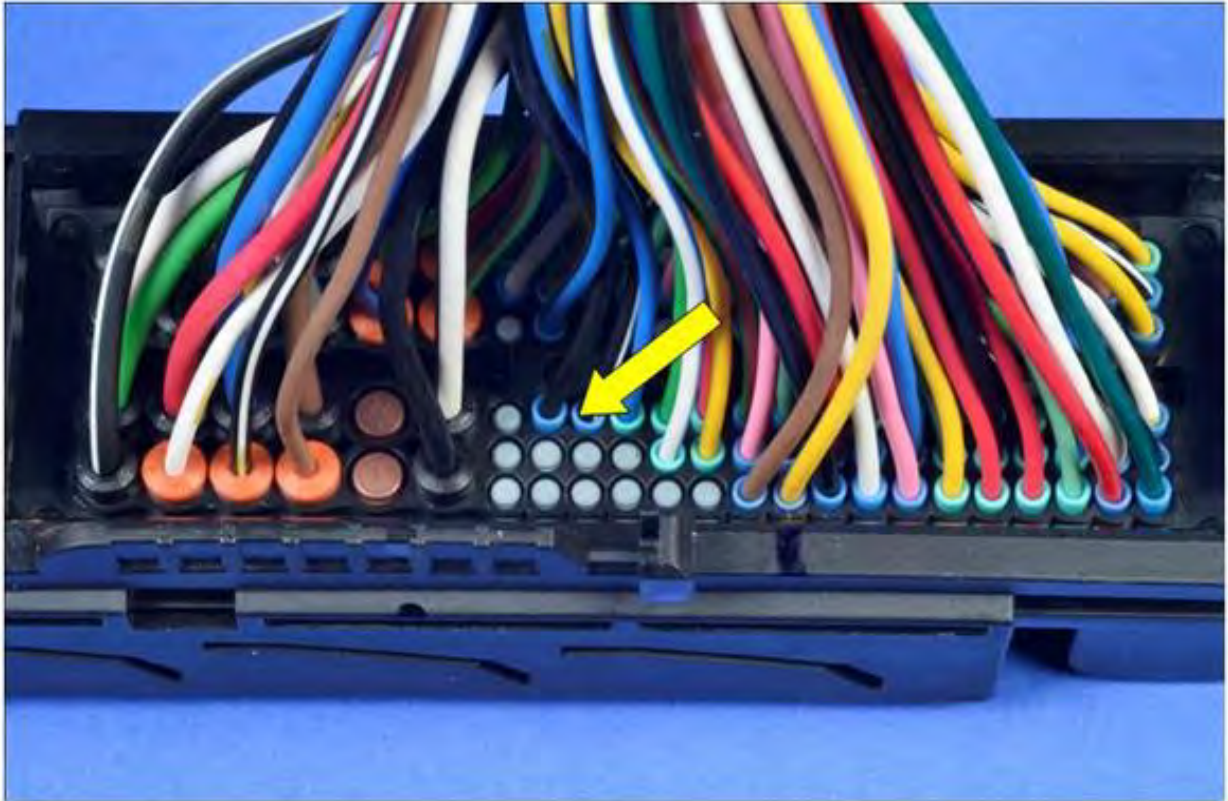


Figure 112. Wiring harness side of female ECM connector. Yellow arrow shows that each connector lead is insulated and protected by a polymeric grommet that helps make the connector waterproof and provides another layer of electrical isolation between sockets.

The male portion of the connector is a molded part attached to the ECM. It has the following characteristics:

- A plastic shell surrounds the pins of the connector, protecting them against direct moisture contact (Figure 113).
- The connector shell has a locking mechanism that interlocks the two-connector portions to prevent connector separation.



Figure 113. Male portion of the ECM connector showing the gold plated and tin plated pins.

10.2.3 Solder and Connector Pins

Prior to the introduction of lead-free solder for 2008 model year vehicles, the connector leads were soldered onto the ECM PCB using SnPb (tin/lead) solder. This was replaced by SnAgCu (SAC) (tin/silver/copper) solder once the Pb-free process was introduced.

The connector pins are copper with a Ni (nickel) underplating and coated with matte Sn for improved soldering. The solder subsumes a majority of the matte tin,¹²⁸ though a small portion of the remaining leads have some exposed matte tin finish. The leads are separated with a spacing that ranges from 1.9mm to 2.2mm for both the waterproof and non-waterproof ECMs.

10.2.4 Wiring Insulation

Each wire of the connector is individually protected by insulation rated for operation in the environment of an automotive engine compartment. Wires are bundled together and wrapped in one or more layers of protective sheathing such as tape and convoluted split loom tubing. To cause wire-to-wire shorting would require a breach of the protective sheathing and individual

¹²⁸ The connector pins on some 2002 to 2006 model year Camry vehicles were coated with bright tin-lead.

wire insulations, and a mechanism to cause an electrical connection between the wires with the breached insulation. This is an unrealistic failure condition due to the characteristics of the insulating materials and the routing of the wires.

If the wiring insulation were to be compromised, evidence of such an event would persist. Exponent has performed electrical measurements on the wiring of vehicles reported to have experienced unintended acceleration; no evidence of a compromise of the insulation has been observed.

10.3 Accelerator Pedal

The accelerator pedal connector contains six pins.¹²⁹ These include the following:

- Four pins that provide DC power to the two independent sensors
- Two pins that carry the output signal from the two independent sensor circuits.

This configuration is applicable for all pedal connectors.

10.3.1 Connector

Figure 114 and Figure 115 show the pin configuration of the potentiometer pedal (male) connector and the Hall Effect sensor pedal (male) connectors. The connector pins labeled ‘VCPA’ (or VCP1) and ‘EPA’ (or EP1) provide the dc power and ground for the primary potentiometer circuit or for the primary Hall Effect sensor (VPA1). Similarly, the connector pins labeled ‘VCP2’ and ‘EPA2’ provide the dc power and ground for the monitoring potentiometer circuit or for the monitoring Hall Effect sensor (sensor output VPA2).

¹²⁹ The first generation of ETCS-i systems had the accelerator pedal position sensors mounted on the throttle body and connected to the pedal by a cable. These sensors had four pins: two outputs, VPA1 and VPA2, a common voltage supply and a common ground circuit.

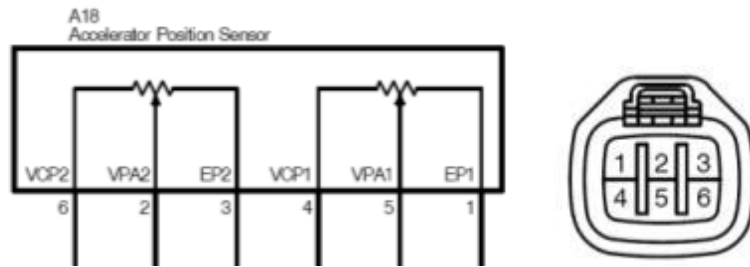


Figure 114. Potentiometer pedal (male) connector.

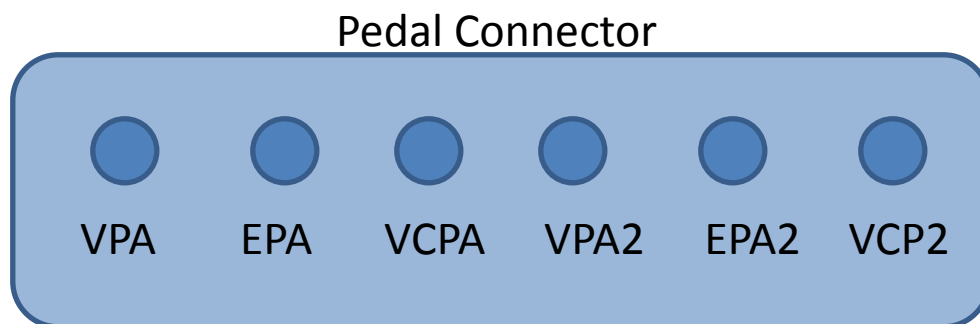


Figure 115. Hall Effect sensor pedal (male) connector configuration.

Figure 116 and Figure 117 show the potentiometer pedal connector and the Hall Effect pedal connector and the wiring harness that connects the pedal to the ECM. The accelerator pedal connector is constructed in two halves: the male portion which is attached to the accelerator pedal, and the female portion which is attached to the connecting wire harness.



Figure 116. Potentiometer pedal connector. Each connector lead is insulated and protected by a polymeric grommet (red arrow) that helps make the connector waterproof and provides another layer of electrical isolation between sockets. Another polymeric grommet seals the two halves of the connector (yellow arrow). The female connector pin receptacles are recessed. There are two barriers surrounding the VPA1 and VPA2 pins (green arrows).



Figure 117. Hall Effect pedal connector. Each connector lead is insulated and protected by a polymeric grommet that helps make the connector waterproof and provides another layer of electrical isolation between the sockets.

Some features of the accelerator pedal connectors include:

- The pedal connector is waterproof. A polymeric seal exists on the female portion of the connector and around each lead.
- The connector has a locking mechanism to prevent inadvertent disengagement.
- The pedal connector is located within the passenger compartment of the vehicle, underneath the dashboard and away from the pedal pads. This location limits the exposure of the connector to damage, moisture and other contaminants. Each pin fits into its own insulated slot to electrically isolate pins from each other.

Figure 118 shows the two halves of the Hall Effect connector. This connector cannot be separated without the disengagement of an interlocking clasp (indicated by red arrows in Figure 118). When separated, the connector's two halves reveal features of the connector, which include a protective shell, polymer gaskets, insulated wires, and recessed pins. The connector is also designed to waterproof standards, so incidental moisture will not reach the conductors. A connector was potted and sectioned to enable viewing the connector design while it was still mated (Figure 119). Note that insulating barriers seal and protect wires from where they enter the connector to where they exit the connector.



Figure 118. Pedal Assembly Connector- female (left) and male (right). Blue arrow shows the gasket. Red arrows show the interlocking clasp.

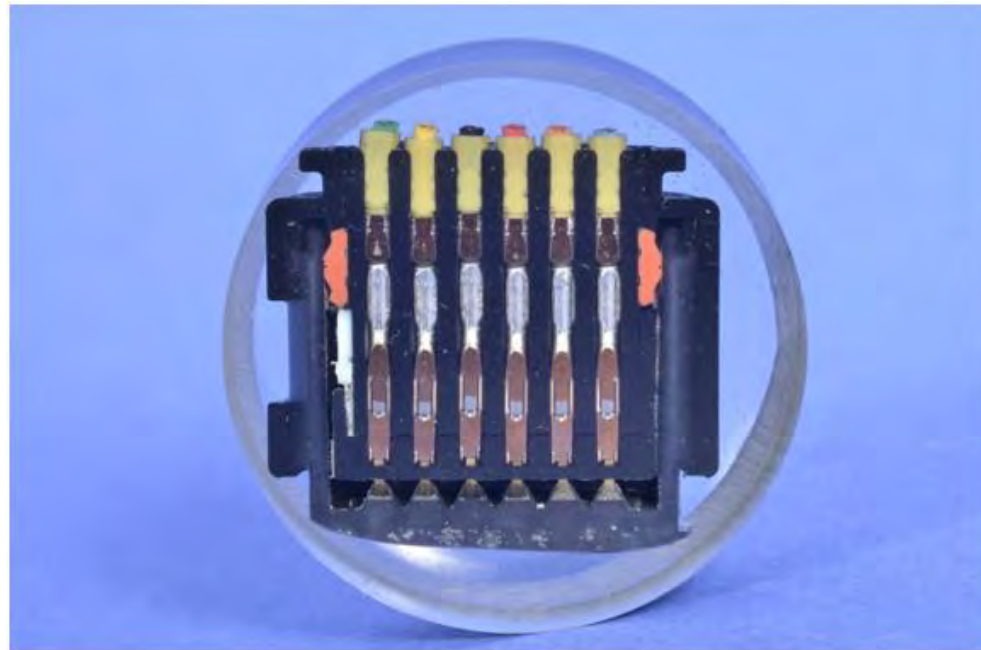


Figure 119. Potted and sectioned Hall Effect based accelerator pedal sensor connector.

The female portion of the connector is comparable in construction to the ECM connector and has similar features. The connector is designed:

- With a plastic shell surrounding the housing of the male portion of the connector to prevent direct moisture contact
- With a rubber gasket that surrounds the rim of the female portion making the connector waterproof
- Such that each pin fits into its own insulated slot to electrically isolate pins from each other
- With recessed pin sockets that reduce the possibility of electrical interconnection between adjacent pins

- With a plastic divider that extends into the connector, further reducing the possibility of electrical interconnection between adjacent pins
- With insulation on each connector lead
- Such that a polymeric grommet provides protection to each connector lead to make it waterproof and to provide additional electrical insulation (Figure 120)
- Such that the wires are spaced to prevent adjacent wire contact.



Figure 120. Each connector lead is insulated and protected by a polymeric grommet that helps make the connector waterproof and provides another layer of electrical isolation between sockets.

The male portion of the connector is a molded part attached to the pedal assembly. It has the following characteristics:

- A plastic shell that surrounds the pins of the connector protecting them against direct moisture contact
 - The connector pins are located on a raised pedestal
 - The connector shell has a locking mechanism that interlocks the two-connector portions to maintain a seal and prevent connector separation.

Another connector design is also used on Hall Effect sensor-based accelerator pedals for some Toyota vehicle models. This connector design is shown in Figure 121. The connector design is waterproof, and has similar features as discussed previously, including interlocking plastic shells surrounding the male and female halves, individual grommet seals for each wire, a polymeric seal between connector halves, recessed sockets between pins, plastic separators between pins on the female half, plastic ribs between pins on the male half, and wire spacing to prevent adjacent wire contact.



Figure 121. Accelerator pedal connector design used on certain models showing certain features, such as individual wire polymeric grommet seals, polymeric seal between connector halves, and interlocking connector.

10.3.2 Wiring Insulation

The wiring from the accelerator pedal is bundled and wrapped or placed inside a plastic conduit (called convoluted split loom tubing). The wiring bundle is packaged and routed in a manner that protects the insulation from compromise. Despite the protection against such an event,

were the wiring insulation to be mechanically compromised, evidence of such an event would persist.

The individual electrical wires are insulated with PVC (polyvinyl chloride) insulation that is rated to the Japanese Automobile Standard Organization (JASO) D 608-92. The wire specifications require that the wire not be damaged when subjected to a variety of tests, including a “withstand voltage” test where 1,000 volts are applied to the cable while fully immersed in water. Under normal operating conditions, these wires are connected to a relatively low voltage of 5 Vdc. A compromise of the wires’ insulating capacities due to dielectric breakdown at such low voltages and in the operating environment inside a vehicle is unrealistic.

10.4 Throttle

There are two types of throttle connectors. One type has a connector with four pins for the throttle sensors and a separate two-pin connector for the motor control. The other type of connector consists of the four pins for the throttle sensors and the two pins for the motor control integrated into a single connector. The throttle body connector with six pins has the following connections:

- Two pins that provide the PWM signals to drive the throttle motor that opens and closes the throttle valve.
- Two pins that provide dc power to the two independent Hall Effect sensors that detect the position of the throttle valve (i.e. VCTA and ETA).
- Two pins that connect to the output of the circuits (i.e. VTA1 and VTA2).

The throttle connector with four pins has the same characteristics as described above but lacks the two motor control pins. Most throttle bodies, including the throttle bodies that utilize the Hall Effect based sensor technology use a six-pin connector. Examples of vehicles with the four-pin connector include the 2002 and the 2003 V6 Camry.

10.4.1 Connector

Figure 122 shows the throttle body connector of a 2007 Camry throttle assembly. The connector pins 'VCTA' and 'ETA' (see Figure 122) provide the dc power and ground respectively, for the two Hall Effect sensors. The connector pin labeled 'VTA1' provides the Hall Effect output feedback signal. The connector pin labeled 'VTA2' provides the Hall Effect output signal for the monitoring Hall Effect sensor. The connector pins labeled M+ and M- provide the PWM signals to the throttle motor.



Figure 122. Connector pins on the throttle body connector. From left to right: VTA1, VCTA, VTA2, ETA, M+, M1. The signal pins are gold plated.

The connector, when in service and when mated to the female connector on the throttle body, is located within the engine compartment. The two halves of the connector are locked by an interlocking clasp that prevents inadvertent disengagement. When separated, the connector's two halves reveal features of the connector, which include a protective shell, polymer gaskets, insulated wires, and recessed pins.

The male portion of the connector (Figure 123) has features similar to the male portion of the connectors on waterproof ECMs. Plastic shells, locking mechanisms, etc., provide additional insulation to the connector pins and prevent faults from developing on the connector. In

addition, the connector consists of four gold plated pins for the signal and two tin plated pins for the power terminals.



Figure 123. Male portion of the throttle body connector with gold plated signal pins and tin plated power pins.



Figure 124. Close-up of female portion of the throttle body connector with the orange sealing grommet visible.

The female portion of the throttle body connector is shown in Figure 124 and is comparable in construction, with features similar to the female portion of one of the accelerator pedal connector designs, including a plastic shell surrounding the housing of the male portion of the connector, recessed pin sockets, etc. Similar to the male portion of the throttle body connector,

the female throttle body connector also consists of four gold plated pins for the signal and two tin plated pins for the power terminals.



Figure 125. Each throttle body connector lead is insulated and protected by a polymeric grommet that helps make the connector waterproof and provides another layer of electrical isolation between sockets.

10.4.2 Wiring Harness

Just as with the wiring connected to the accelerator pedal, the wiring from the throttle body is bundled, and placed inside a plastic conduit (called convoluted split loom tubing). The wiring includes a shield around the motor M+ and M- conductors to prevent them from causing EM interference in the signal wires. The throttle position sensors are powered by a two-conductor twisted pair on VCTA and ETA for increased noise immunity. As discussed in preceding sections, if the wiring insulation were mechanically compromised, evidence of such an event would persist.

11 Additional Issues

11.1 2007 Camry Engine “Hesitation” Complaints

Some drivers of 2007 L4 5-speed Camry vehicles complained about a hesitation phenomenon when trying to accelerate the vehicle, especially during vehicle start-up from a stationary condition. The complaints described a lack of response from the vehicle as the accelerator pedal was pressed. Under certain conditions, the vehicle response lagged the pedal depression by several seconds. The NHTSA complaint data contains dozens of complaints on this speed control issue.

Some drivers might respond to this delay by depressing the accelerator pedal further. When the engine and power train respond, often by downshifting and changing the engine operating conditions, the result can be greater acceleration than the driver originally intended.

The source of this lag in engine response is related to the design of the knock-control ignition timing system. Ignition timing refers to the time when the spark is triggered relative to the piston position. Controlling the ignition timing allows for the optimization of various vehicle parameters including fuel economy, engine performance, engine knocking etc. The ECM uses multiple signals, including those from a knock control sensor, to determine ignition timing and to prevent or minimize knock.

Knock occurs when the fuel-air mixture ignites too rapidly and detonates in localized pockets within the combustion chamber, resulting in a knocking, rattling or pinging sound. Knock, if it occurs over a prolonged period of time, can cause permanent and expensive damage to the engine. There can be many causes for knock, including low octane fuel, problems with the EGR system, or an overheating engine.

The purpose of the knock sensor is to sense detonation pulses when they occur and to transmit this information to the ECM. The ECM responds by retarding the ignition timing. Retarding the spark timing delays the introduction of the spark into the combustion chamber, reducing the

propensity for knock. The side effect of retarding the spark timing from optimal (in the absence of knock) is reduced engine torque, which the driver would notice as a delay in acceleration.

For the 2007 L4 5-speed Camry vehicles, the ignition timing retardation to prevent knock depends on feedback from the knock sensor input and a knock correction learning value. The knock correction learning value can be regarded as a calibration factor. The number of degrees of ignition timing retardation was calculated in the ECM by adding the knock correction learning value to the retardation value determined using input from the knock sensor.

The cause of the hesitation in the 2007 L4 5-speed Camry vehicles was due to the algorithm used to calculate the knock correction learning value, which resulted in more ignition timing retardation than was necessary to prevent knock. A software change was implemented to improve engine performance. The software was revised to use a more sophisticated algorithm for calculating the knock correction learning value that depended on additional engine operating conditions. The software update mitigated the vehicle hesitation issue. Affected vehicles were the 2007 and early 2008 model year 4-cylinder Camrys with the 5-speed transmission.

11.2 Stalling of Corolla/Matrix Vehicles

Toyota issued a voluntary recall of 2005 to 2008 model year Corolla and Matrix vehicles in August 2010. This section discusses and describes the root cause of the ECM related problems that lead to this recall.

The root cause of the problems stemmed from uncured conformal coating on the ECM, resulting in thermo-mechanical stress, and a manufacturing defect of certain components (varistors) on the ECMs of these vehicles. The uncured conformal coating also resulted in stresses on the solder joints of some components on the ECMs. The uncured conformal coating resulted in high thermo-mechanical stresses on the pins of the Main processor. An analysis performed to determine the consequences of a failure of the pins on the Main processor indicated one of the following possible responses:

- Stalling of a running engine
- Inability to start a vehicle
- MIL turning on and DTC set
- No effect on vehicle operation.

The analyses did not identify any scenario where the possibility of open-circuit failure of the Main processor pins would result in UA.

11.3 Brake Override Systems

In the NPRM, the NHTSA defines a brake override system (BOS)¹³⁰ as:

“an electronic function of the engine control system. Generally, it works by continuously checking the position of the brake and accelerator pedals and by recognizing when an acceleration command through the accelerator pedal is in conflict with a concurrent application of the brake pedal. If the BTO system identifies that a pedal conflict exists, it invokes the override function which causes the engine control system to ignore or reduce the commanded throttle input, thus allowing the vehicle to stop in a normal fashion.”

A BOS generally works by checking the position of the brake and accelerator pedals and recognizing when an acceleration command through the accelerator pedal is in conflict with a concurrent application of the brake pedal. If a pedal conflict is identified, the override functionality is activated. Typically, the BOS may check several vehicle parameters, such as vehicle speed, accelerator pedal position, brake pedal position, pedal sequence, and engine RPM to determine if there is a conflict. The BOS is also designed to ensure minimal interference with normal vehicle operation (e.g. accelerating from a stop on a slope).

¹³⁰ Also called the Brake–Throttle Override (BTO) system.

11.3.1 BOS Implementation

As BOS is implemented in proprietary vehicle software, it is typically not possible to determine which vehicles have BOS from vehicle service manuals or vehicle inspections. To determine manufacturer implementations of BOS, press releases from the manufacturers and news articles were utilized to create Table 20. As Table 20 shows, a majority of vehicle manufacturers in the US did not implement BOS across their model lineup prior to the 2011 model year. However, the technology was rapidly deployed starting with the 2012 model year vehicles.

Table 20. Vehicles with BOS

Make/Model Yr	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Chrysler												All except PT Cruiser			
Dodge															
Jeep															
Ford													Almost 100%		
Mercury															
Lincoln															
GM															
Buick															
Cadillac										STS-V 08+ & CTS-V 09+					
Chevrolet	Corvette 97+, Cobalt 05+, HHR 06+, Malibu I4 08+, Colorado V8 09+, Camaro 10+														
GMC											Canyon V8				
Hyundai												All veh manf > Feb 20 2010 except Elantra & Accent			
Honda															
Acura															
Mazda													Mazda 2-y		
Nissan															
Infiniti															
Subaru														Impreza 2.0i	
Toyota												85%-y			
Scion															
Lexus															
BMW															
Mercedes															
VW															
Audi															
	Legend														
	Not on any models														
	On some models														
	On all models with automatic transmissions and gasoline engines														

11.3.2 BOS Characterization Tests¹³¹

Testing was performed to characterize the operation of the BOS in selected non-Toyota vehicles. The following four Toyota Camry peers known to have BOS were selected for the tests:

- 2008 Nissan Altima
- 2010 Dodge Avenger
- 2008 VW Passat
- 2010 Chevy Malibu.

The vehicles were instrumented to collect the following during the tests:

- Accelerator pedal position¹³²
- Applied brake pedal force (lbs.)
- Brake lamp switch status
- Vehicle speed (mph)
- Engine speed (rpm)
- Throttle valve angle.¹³³

¹³¹ Details of the test setup and data are included in Appendix H.

¹³² Measured as a % of full pedal depression.

¹³³ Measured as a % of wide open throttle.

Tests were performed to characterize the operation of the BOS. The following tests were performed:

- Required brake pedal force for BOS activation
- BOS activation with application of brake pedal before accelerator pedal
- Vehicle speed threshold for BOS activation
- BOS activation time delay, accelerator pedal position and throttle request angle

11.3.2.1 Required Brake Pedal Force for BOS Activation

The aim of this test was to determine if the activation of the BOS was a function of the applied force on the brake pedal. The test results are as shown in Table 21.

Table 21. BOS activation and applied brake pedal force

Vehicle	Brake Force Impact on BOS operation
2008 Nissan Altima	None
2010 Dodge Avenger	None
2008 VW Passat	None
2011 Chevrolet Malibu	Yes ¹³⁴

The brake pedal was applied after the accelerator pedal during the test runs. Testing indicated that under the tested conditions, the applied brake force did not have an impact on BOS activation for all tested vehicles except the Malibu¹³⁵.

¹³⁴ With 100% pedal depression and the vehicle at 40 mph, BOS activation occurred if the brake force was greater than approximately 30 lbs.

¹³⁵ The Malibu brake pedal contained a potentiometer which measured the brake pedal position which was likely used as an input in the determination of the BOS activation.

11.3.2.2 BOS Activation with Application of Brake before Accelerator Pedal

The aim of this test was to determine if the activation of the BOS was dependent on the order of pedal application. The test was performed at vehicles speeds of approximately 30 miles per hour with the accelerator pedal depressed completely. The test results are as shown in Table 22.

Table 22. BOS activation and order of pedal depression

Vehicle	BOS Activation (Brake pedal applied first)
2008 Nissan Altima	Yes
2010 Dodge Avenger	No
2008 VW Passat	No
2011 Chevrolet Malibu	Yes

Testing indicated that the BOS in the Avenger and the Passat did not activate if the brake was applied before the accelerator pedal. However, for the Altima and the Malibu¹³⁶, the order of brake application was not a factor in the activation of the BOS.

11.3.2.3 Vehicle Speed Threshold and Accelerator Pedal Position

The aim of this test was to determine if the activation of the BOS was dependent on vehicle speed and the amount of accelerator pedal depression. The test results are shown in Table 23.

Table 23. BOS activation and vehicle speed threshold

Vehicle	Speed Threshold for BOS Activation (mph)	Vehicle Speeds Tested ¹³⁷ (mph)	Accelerator Pedal Depression during Test (%)	Brake Force during Test (lb)
2008 Nissan Altima	5	0–60	100	Not an input
2010 Dodge Avenger	5	5–55	100	Not an input
2008 VW Passat	0	5–55	100	Not an input
	~5	~5–10	25–30	
2011 Chevrolet Malibu	0	~5–40	100	~30–70
	~10–20	~10–50	~25–35	~25–55

¹³⁶ Since brake force impacts the activation of the BOS on the Malibu, the applied brake force was 30 lb during the tests.

¹³⁷ Approximate values

Testing indicated that the:

- Vehicle speed thresholds for the activation of the BOS was different for the tested vehicles.
- Activation of the BOS was not a function of the amount of accelerator pedal depression for the Altima, Passat and Malibu. However, the BOS on the Avenger did not activate if the pedal depression was less than approximately 80%.

11.3.2.4 BOS Activation Time Delay, Accelerator Pedal Position, and Throttle Request Angle

The aim of this test was to determine the time delay in the activation of the BOS and to characterize the effect of the activation of the BOS on the throttle opening angle. The test results are as shown in Table 24.

Table 24. BOS activation time delay, accelerator pedal position and throttle request angle

Vehicle	% Throttle Opening after BOS Activation	Time Delay for BOS Activation(s)	Approximately Vehicle Speed (mph)	Accelerator Pedal Depression (%)	Applied Brake Force (lb)
2008 Nissan Altima	~40	<1	5–60	100	Not a factor
2010 Dodge Avenger	5	~2	5–55	100	Not a factor
	Did not activate		30–35	45–80	
2008 VW Passat	5	~2	15–55	100	Not a factor
			30	60	
			5–10	25–30	
	30	~0.5–1.5	5–10	100	
2011 Chevrolet Malibu	Throttle closes	~0.5–1.5	20–40	20–65	25–50
	50	~3–5.5	35–40	100	35–50
	75	~1	10	100	65
		< 1	3–10	100	60–70

Testing indicated that:

- The time delay in the activation of the BOS varied significantly among the tested vehicles. In addition, the time delay for the activation of the BOS was a function of vehicle speed for the Malibu.
- BOS activation did not reduce the throttle opening angle to its value at idle in all tested vehicles. Activation of the BOS:
 - Reduced the throttle to an opening angle of approximately 40% for the Altima.
 - Reduced the throttle to an opening angle of approximately 5% for the Avenger (close to the throttle opening when the vehicle is at idle).
 - Resulted in a reduction in the throttle opening angle. The magnitude of the reduction was a function of the vehicle conditions at the time of activation for the Malibu and the Passat.

11.3.3 Summary

A review of the marketplace and testing performed on vehicles indicated the following:

- BOS implementation was not universally employed in vehicles equipped with ETC and was implemented in a small number of vehicles prior to model year 2011. Most manufacturers that had at least one vehicle with BOS prior to 2011 had not implemented the system across their fleet.
- Testing indicated that BOS is an evolving technology with different variations employed by different vehicle manufacturers. These differences include the vehicle speed at which BOS activates, the time delay in activation, the required acceleration pedal position for activation and the reduction in engine torque once BOS is activated.

- Testing also indicates that implementation of the BOS requires sophisticated algorithms in the ETCS-i, that monitor a number of signals and vehicle conditions used as criteria for activating the BOS.

12 Summary

Exponent investigated whether Toyota vehicles equipped with electronic throttle control technology could accelerate without driver input. The Toyota Camry was selected for the detailed study because Exponent's analysis of unintended acceleration complaints in NHTSA's database found elevated rates of such complaints and the vehicles had been the subject of multiple NHTSA investigations. As part of the analysis, Exponent reviewed the software and hardware of Toyota Camry vehicles with ETCS-i systems and performed testing on Camry and other Toyota vehicles.

The analysis performed by Exponent identified the various subsystems of the ETCS-i system and identified failure modes associated with each of the subsystems and the response of the vehicle to faults in these sub-systems. Testing both in the laboratory and on vehicles was used to analyze and study the operation of both the hardware and the software systems. Exponent's analysis found the following:

- The vehicle's electronics, software and overall system design employ a network of protection designed and incorporated in the vehicle that transitions the vehicle to one of the designed fail-safe modes in the event the engine control module (ECM) detects a sub-system or component failure.
- Exponent's evaluation and testing determined that realistic environmental levels of electromagnetic interference (EMI) would not cause UA in Toyota vehicles. The vehicles' electronics and software employ multiple strategies that minimize interference from electrical noise and mitigate its possible consequences.
- "Latch-up" was eliminated as a potential root cause for reported incidents of unintended acceleration. The multiple levels of protection in the ETCS-i and its network of safety, that include electronics, software, and the use of silicon-on-insulator technology in many integrated circuits, prevent latch-up (if it could occur) from resulting in UA.

- The system design implements several approaches for mitigating concerns associated with either the formation of tin whiskers, or the growth of tin whiskers that are sufficiently long and have the potential for shorting adjacent conductors¹³⁸. These include, among others:
 4. Conformal coating of electrical printed circuit boards. The coating acts as a mechanical barrier against tin whisker growth;
 5. Encasing of certain components in an epoxy potting compound, which also acts as a mechanical barrier against tin whisker growth;
 6. Employment of electrical connections that either do not contain tin, such as gold and nickel-palladium-gold coatings, or that use techniques known to limit whisker growth.
- An analysis of the system level software safeguards indicates that, in addition to the dedicated component level safeguards that monitor and respond to the various subsystem and component malfunctions, system level software safeguards are designed to detect failures of the system and to prevent the vehicle from experiencing UA either due to single-point failures or due to the failure of multiple software modules and/or electronic subsystems. The response of these safeguards was investigated in detail using hardware-in-the-loop-simulations; our results indicated that these safeguards are designed to ensure that the allowable deviation in the throttle opening angle under the simultaneous failure of multiple sub-systems is limited.
- A line-by-line review of the sections of the source code relevant to throttle control was performed to identify possible logical or functional bugs that would result in UA; no such faults were found.

¹³⁸ Only one manufacturer of one type of pedal position sensor had a concern with tin whisker formation. Detailed studies on the response of this sensor, along with reviews of warranty data, could not attribute reported incidents of unintended acceleration to tin whiskers.

- Exponent reviewed the software test documents from Toyota and performed static analysis on source code to identify runtime errors that would result in UA; no such errors were found.
- The analysis and testing performed on components and vehicles indicated that the system design prevents the vehicle from experiencing UA in the event of:
 - Component failures within sub-systems
 - Power supply anomalies such as over-voltage, under-voltage etc.
 - Realistic resistive faults due to contaminants, tin whiskers, etc.

Based on our investigation, Exponent concluded that the electronics and software were not the root cause of the reported incidents of unintended acceleration in the Toyota vehicles we evaluated.

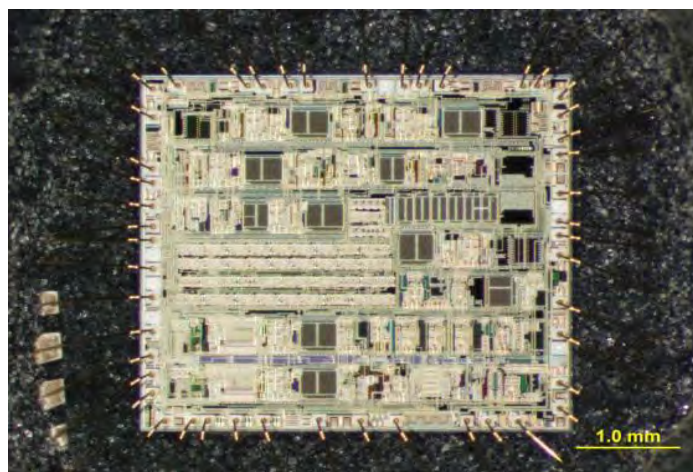
Appendix A. Accelerator Pedal Position Learning

As discussed in section 4.5, the pedal position values learned at ignition on may be updated under certain conditions that can depend on vehicle speed, brake pedal depression, past values of VPA1 etc. Each update of the pedal position learned value cannot exceed approximately 0.02 V. However, if the deviation in value between the original learned value and the new value to be learned exceeds 0.2 V then a flag is set to prevent any updates to the learned values until the ignition is turned off and back on again.

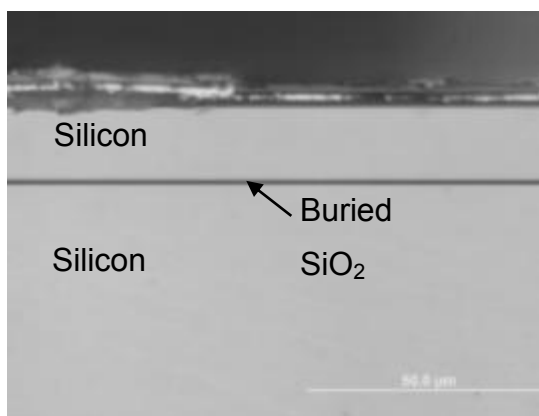
Appendix B. SOI Technology on Toyota ECMs

Power Supply Chips

Three types of power supply ICs were found in the ECMs examined by Exponent. Photographs of the die and cross section images for the three die types are shown in Figure 126, Figure 127, and Figure 128.

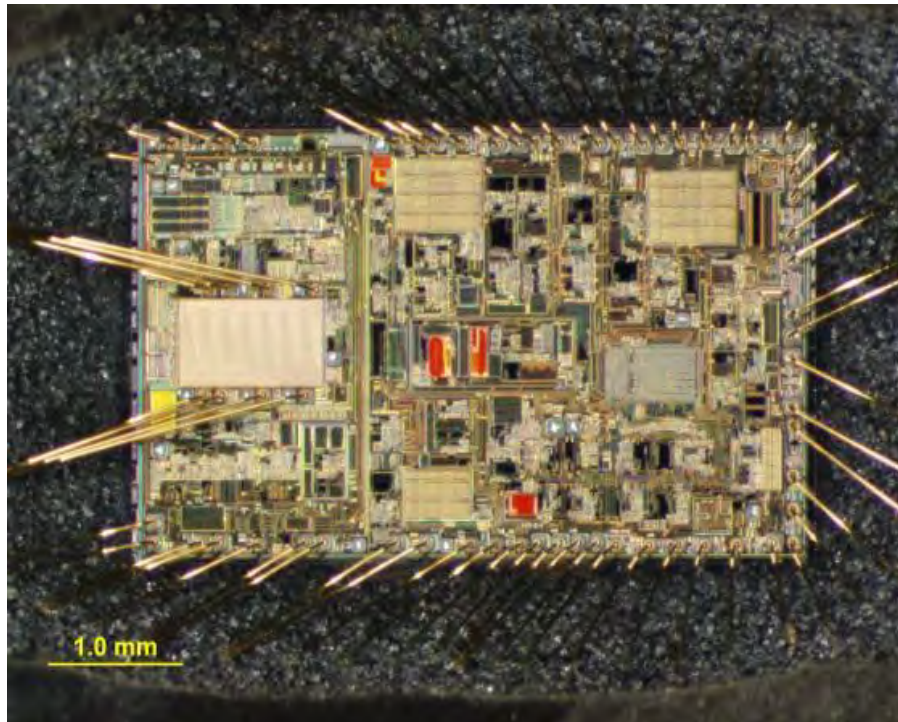


(a) Die Photo

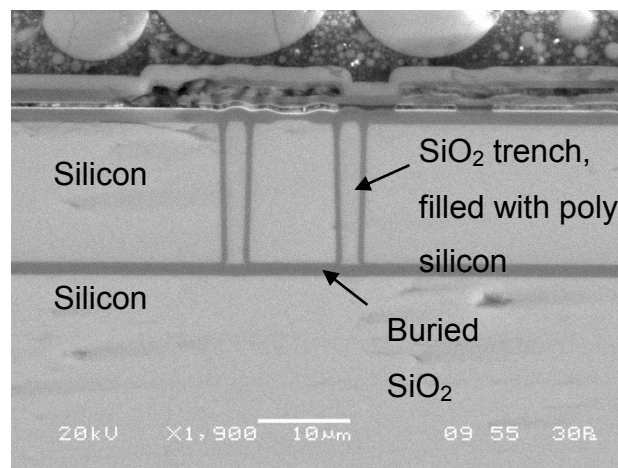


(b) Cross section image

Figure 126. Die photograph and cross section image of die type 1.

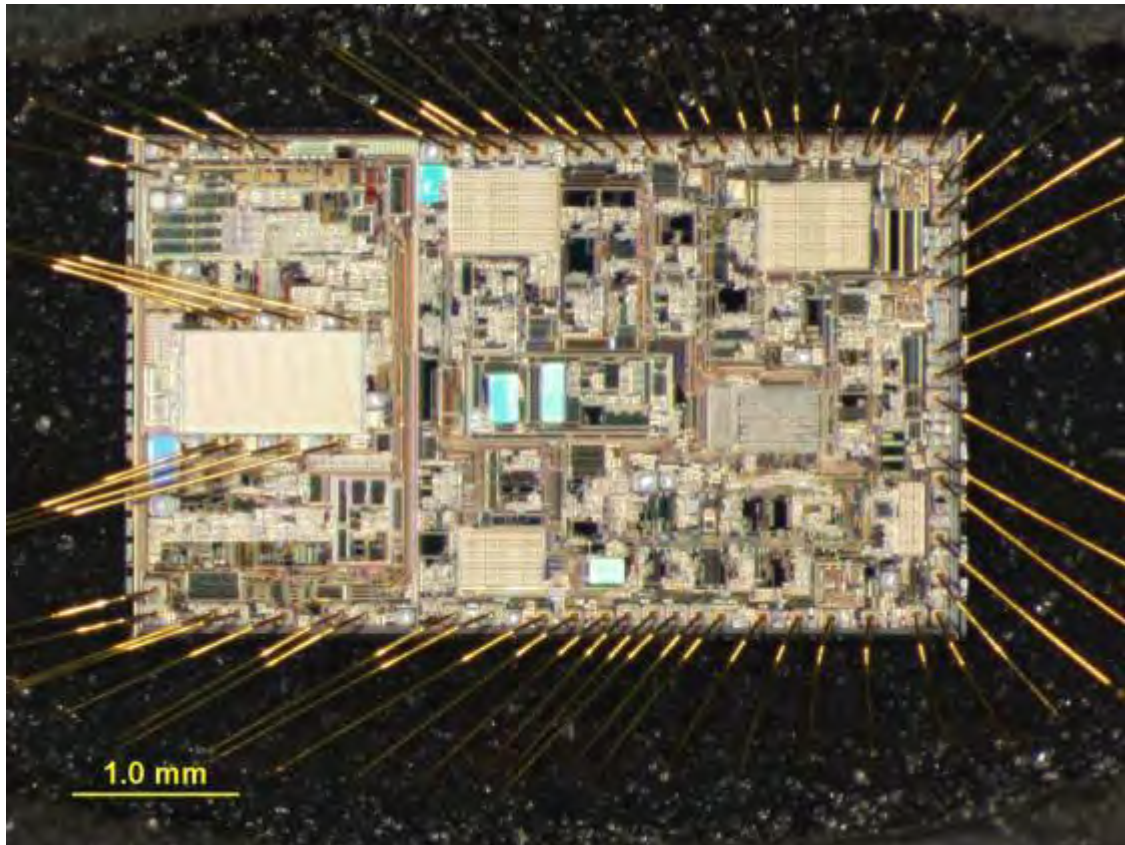


(a) Die photo

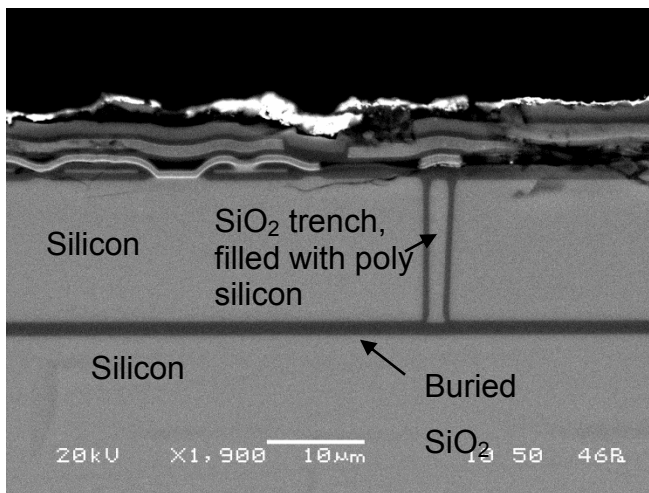


(b) Cross section image

Figure 127. Type 2 die photograph and cross section image.



(a) Die photo

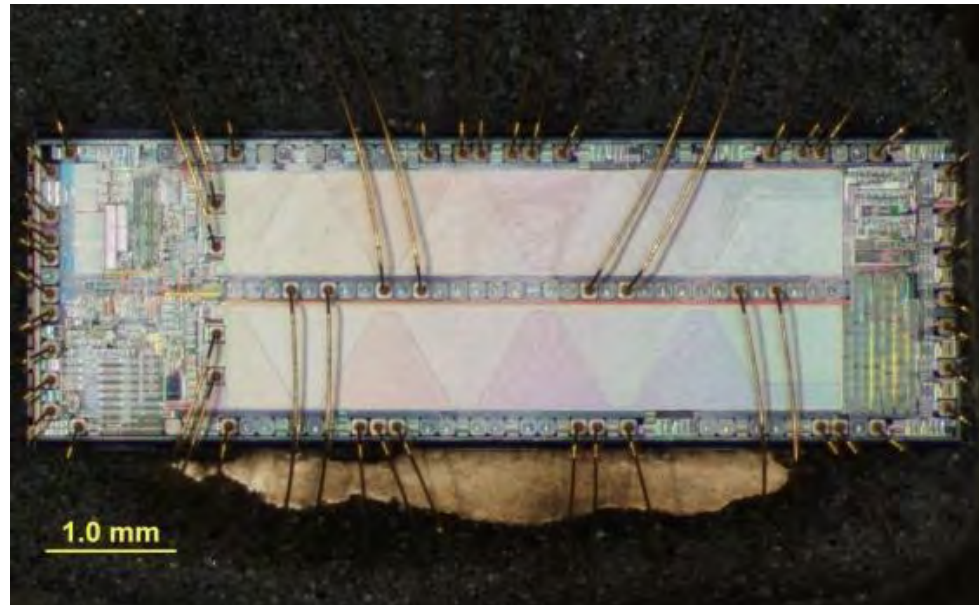


(b) Cross section image

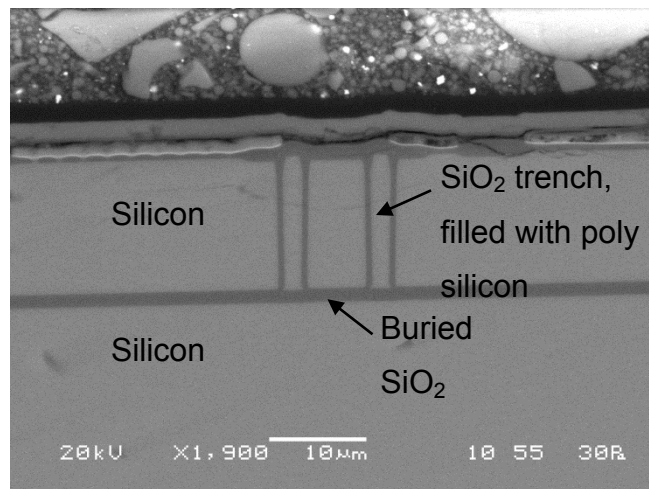
Figure 128. Type 3 die photos and cross section image.

Throttle Motor Driver ICs

Two types of ECM throttle motor driver ICs were examined by Exponent. Photographs of the die and cross section images are shown in Figure 129 and Figure 130.

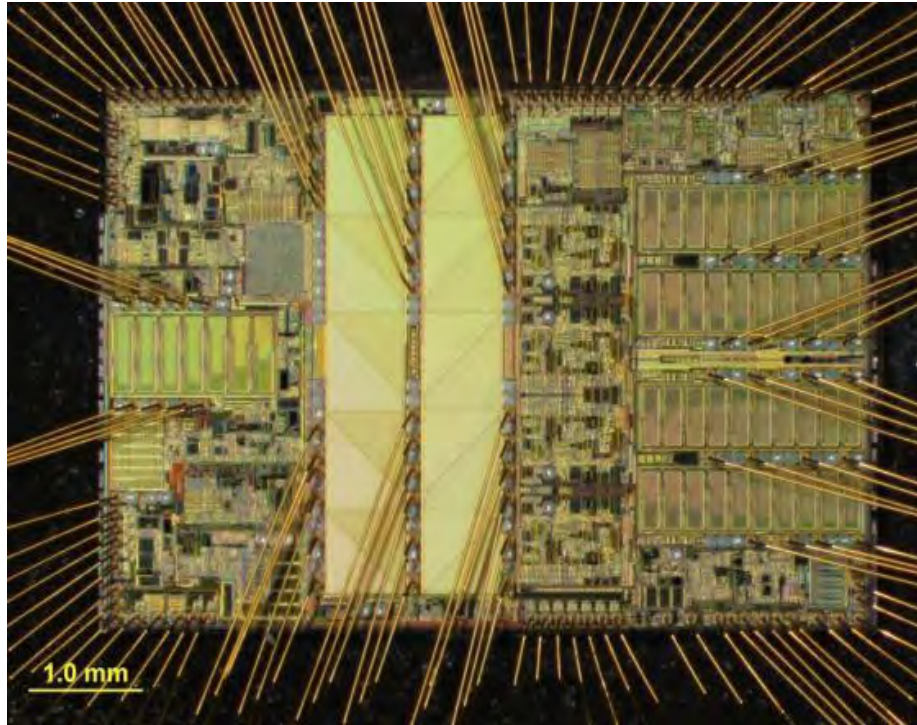


(a) Die photo

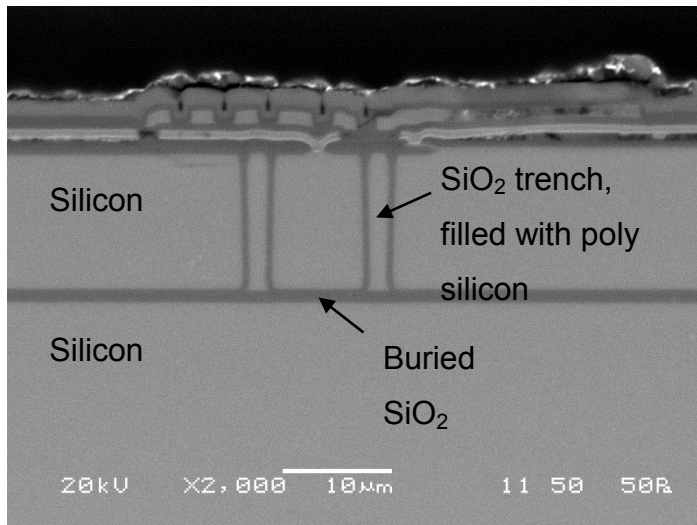


(b) Cross section image

Figure 129. Type 1 die photographs and cross section image.



(a) Die photo



(b) Cross section image

Figure 130. Type 2 die photographs and cross section image.

Appendix C. Latch-up on Delphi ECMs

Delphi ECMs do not use SOI technology for the PWM driver IC. However, starting with the 2010 model year Corolla, the ECM was manufactured by Denso. These ECMs utilize parts that are different from those used on Delphi ECMs.

Even though the ECMs manufactured by Delphi do not utilize SOI technology, the ECM design for the throttle motor driver circuitry utilizes external transistors for the H-bridge circuitry and uses a pre-driver IC to drive the H-bridge transistors. The design of the H-bridge driver circuitry protects against the main source of latch-up: negative voltage spikes. In addition, external components (such as a diode between the 12 V signal and ground) provide protection against negative voltage transients which can also lead to latch-up conditions.

In addition, even if a latch-up condition on the throttle motor driver circuitry was to occur, the system is designed to detect this condition and set a DTC. This is because of the following:

- The ETCS-i system is designed to continuously vary the throttle plate position and hence the throttle opening angle even if the change in the throttle opening position is small.
- If no change in the throttle opening angle occurs, (i.e. a stuck throttle condition), the software system is designed to set a DTC and transition the vehicle to the fail-safe mode.
- If a latch-up in the throttle motor driver circuit occurs, a wide open throttle condition will result. In addition, due to a loss of control of the throttle motor driver circuit and the latch-up condition, no change in the throttle opening position will occur.
- This will trigger the stuck throttle condition flag and result in a DTC (P2111). This DTC will cause the vehicle to transition to the fail-safe mode.

Hence, even though the Toyota Corolla ECMs manufactured by Delphi do not utilize SOI technology the system design ensures that a latch-up condition either on the ECM circuit or on the pedal/throttle Hall Effect sensors will not lead to UA.

Appendix D. Inspection of Field Components

Inspection of Field Components

Appendix E. Pin-to-Pin Short Testing

Short and Open Circuit Testing: ECU Main and Sub-Processors

1. Tests simulating direct and resistive short circuits between adjacent processor pins
("Pin-to-Pin" testing)
2. Tests creating an open circuit on selected processor pins
("Pin Disconnect" testing)

Appendix F. Tin Whisker Risk Assessment

Tin Whisker Risk Assessment for Toyota Camry Models 2002-2009: Engine, Throttle Body, and Accelerator Control Electronics

Appendix G. A/D Converter Testing

Analog to Digital Converter Failure Test

Appendix H. BOS Characterization Tests

Brake Override System (BOS) Characterization