Appendix B – Fishbone Diagrams

(Note that tables and fishbone diagrams are 11x17 layout size)

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

REDACTION NOTE

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

Table of Contents

List of Figures

List of Tables

Ishikawa (Fishbone) Diagrams

The failure fishbone, shown in this Appendix, organizes potential failure causes into a functional hierarchy and was used to identify and disposition each potential cause. The fishbone for this investigation was developed to address hardware and software functional failures, and consequently does not always devolve to the part level. The fishbone, shown in Figure B-1, is configured into 9 major areas: Throttle Function, Pedal function, Cruise Control Function, Idle Speed Control Function, Transmission Shifting and Vehicle Stability Control Function, Software, Environmental Effects, and Mechanical Effects. Elements of Mechanical Effects were included for completeness, but were not part of this study.

While not absolute, in general, the NESC team focused on those failures that could increase the throttle opening, and do not set a DTC. Any failure or set of failures that were identified as potential sources of a UA, without setting a DTC, is discussed in the body of the report in their functional area. This is a subset of all possible failures and does not include design features that intentionally open the throttle or all possible variations of a given failure mode.

Table B-1, unlike the fishbone, divides the potential UA sources for the Throttle Function by category or types of failure conditions such as sensor supply increased resistance or sensor return increased resistance. The fishbone looks at the effects of functional failures, such as Poor Electrical Connection or Wire Damage or Faulty Sensors Power. Within the disposition of the fishbone function, the failure condition is captured as described in Table B-1.

Some failures or sets of failures that were identified as potential sources of a UA are discussed in the body of the report in their functional area. Each major area, shown in the following sections, includes its fishbone diagram and table describing the element dispositions and related system mitigation. The majority of the failure condition, or bones, were dispositioned through analysis and/or test.

Table B-1. Fishbone Summary of Design Sensitivities with Postulated Faults

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

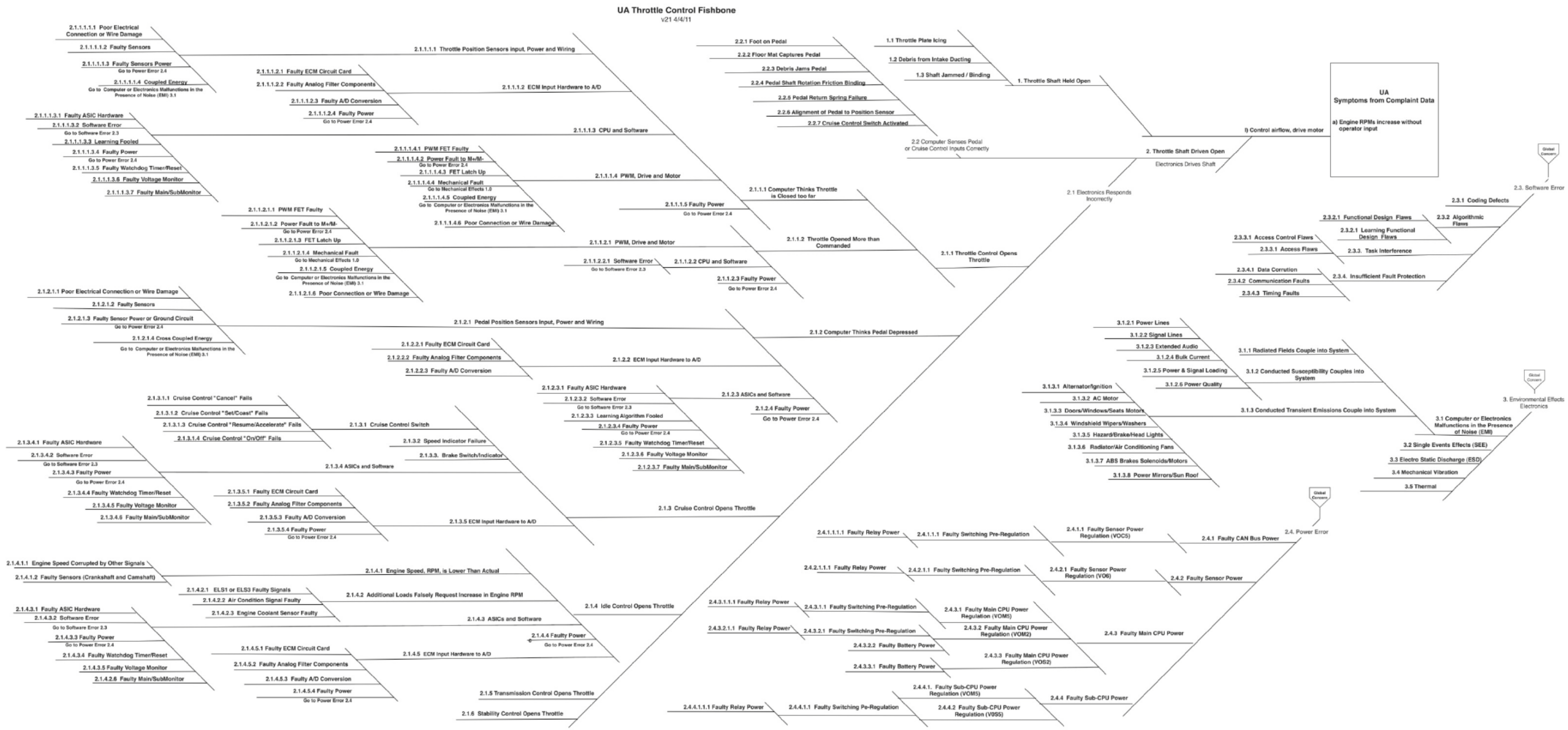

Figure B-1. Full Fishbone Diagram

B-1. Throttle Control Function Fishbone

The Throttle Control Function is the primary control loop and drives the throttle based on inputs from the other five functions. This loop utilizes two throttle position sensors and the inputs from the other functions to generate a throttle command. The command is then sent to the throttle motor that in turn drives the throttle. The throttle consists of the throttle body with its valve, DC motor, two sensors, and interfaces to the ECM and related software. Figure B1-1 is the fishbone for the Throtttle Function only. Table B1-1 lists the dispositions for each element in the fishbone.

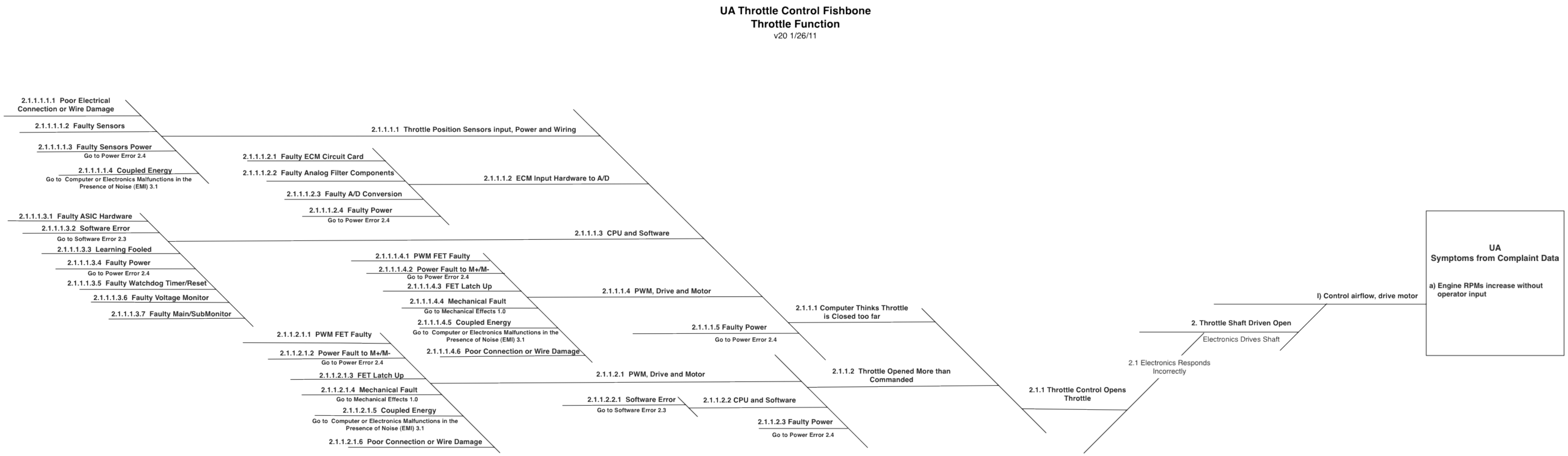

Figure B1-1. ThrottleFishbone Diagram

Table B1-1. Throttle Fishbone Summary of Design Sensitivities with Postulated Faults

Throttle Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
2.1.1.1 Computer Thinks Throttle is Closed too far	2.1.1.1.1 Throttle Position Sensors input, Power and Wiring	2.1.1.1.1.1 Poor Electrical Connection or Wire Damage	VC: A failure mode that causes an increase in resistance to the sensor power, VC, is self-limiting to 3 degrees. This failure mode would cause a drop in VC and, when combined with the learning algorithm, a drop in the sensor output causing the control system to open the throttle to compensate and increase the engine rpm. It is self-limiting as the supply voltage is dropping and the compensating signal cannot be larger than the supply voltage. Some types of Hall Effect sensors' outputs will go to the supply voltage if the supply voltage drops below ~3.7 volts. With resistance above approximately 40 ohms, the failure will be detected and the system will go to a fail-safe mode. Resistive shorts between +5v and Ground is disposition in the Power Element (B-6) and are found to stall the vehicle. Shorting to random signals in the vehicle wiring was not investigated. In the study in the field of connectors within aerospace, conductive contamination causing additional electrical connections in a connector and mechanical wire damage where wires are resistive shorting to chassis or other signals have been observed.	DTC for sensors not within the valid range. DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold Disable Throttle #3 Slightly above Idle Mode Power Off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
			Return: An increase in resistance on the sensor power return line can result in a throttle increase of approximately 1 degree. The learning algorithm will learn the increased input signal caused by the resistance and, when the resistance is removed, the control loop will compensate by increasing the throttle opening. Shorting to random signals in the vehicle wiring was not investigated. In the study in the field of connectors within aerospace, conductive contamination causing additional electrical connections in a connector and mechanical wire damage where wires are resistive shorting to chassis or other signals have been observed.	DTC for sensors not within the valid range. DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.1.1.2 Faulty Sensors	Potentiometer type: Poor electrical contacts resulting in simultaneous poor contact in both independent sensors would be required to prevent detection and tripping a DTC. A high resistive connection at the pot wiper would result in a voltage increase and the throttle closing. Resistive shorts of VTA1 to power result in closing the throttle; resistive shorts to ground on VTA1 might result in opening of the throttle up to 3 degrees.	DTC for sensors not within the valid range. DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
			Hall Effect: A high resistive connection downstream of the Hall sensor output would result in a voltage increase and the throttle closing. Resistive shorts of VTA1 to power result in closing the throttle; resistive shorts to ground on VTA1 might result in opening of the throttle up to 3 degrees. No DC magnetic source was identified near the throttle, which could cause a faulty sensor signal that would last for several seconds or minutes and then disappear. The Earth's magnetic field is orders of magnitude too weak to perturb the sensor signal. Failure of Hall sensor internal circuitry is mitigated by comparison to the second sensor. Maximum throttle opening due to perturbation from magnetic field internal faults of the sensor would be limited to 3 degrees before setting a DTC.	DTC for sensors not within the valid range. Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.1.1.3 Faulty Sensors Power	VC: A failure mode that causes an increase in resistance to the sensor power, VC, is self-limiting to 3 degrees. This failure mode would cause a drop in VC and, consequently, a drop in the sensor output causing the control system to open the throttle to compensate and increase	DTC for sensors not within the valid range. DTC Position does not match commanded Disable Throttle #3 Slightly above Idle Mode

Throttle Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
			the engine rpm. It is self-limiting as the supply voltage is dropping and the compensating signal cannot be larger than the supply voltage. Some types of Hall Effect sensors' outputs will go to the supply voltage if the supply voltage drops below ~3.7 volts. With resistance above approximately 40 ohms, the failure will be detected and the system will go to a fail-safe mode.	Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
			Return: An increase in resistance on the sensor power return line can result in a throttle increase of approximately 1 degree. The learning algorithm will learn the increased input signal caused by the resistance and, when the resistance is removed, the control loop will compensate by increasing the throttle opening.	DTC for sensors not within the valid range. DTC Position does not match commanded Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.1.1.4 Coupled Energy	Throttle sensor component level testing with current injection in both VTA signals noted an engine rpm increase at various frequencies from 125Hz to 10KHz. At a 500Hz sine wave aliasing was observed between the input signal and the throttle output. There are two Technical Field Reports (TQCN/TOY-RQ-00074023_FTR-7QR101241 and TQCN/TOY-RQ-00074046_FTR-7QK101441A) documenting unknown coupling to VTA traced to the E8 ground splice. One field report (TQCN/TOY-RQ-00074514) documented an unknown spike coupling to VTA resulting in a 100 rpm engine surging. See EMI branch 3.1 Coupling of the M+ into the VTA signal was not indicated by a comparison of six complaint vehicles with two non-complaint vehicles. Measurements of the 6 complaint vehicles did not indicate a higher coupling of M+ into the VTA signals than the 2 non-complaint vehicles.	DTC for sensors not within the valid range. DTC Position does not match commanded Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
	2.1.1.1.2 ECM Input Hardware to A/D	2.1.1.1.2.1 Faulty ECM Circuit Card	Poor solder joints or cracked traces could result in an increased resistance that would decrease both VTA's resulting in an increase in throttle opening, as covered in 2.1.1.1.1.1 Poor Electrical Connection or Wire Damage. The failure would be self-limiting as the supply voltage is dropping and the compensating signal cannot be larger than the supply voltage or result in a throttle increase of approximately 3 degrees.	DTC for sensors not within the valid range. DTC Position does not match commanded Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.1.2.2 Faulty Analog Filter Components	Cracked or damaged passive components could result in an increased series resistance that would increase both VTA's resulting in a decrease in throttle opening, as covered in 2.1.1.1.1.1 Poor Electrical Connection or Wire Damage. Changes in the cutoff frequency of the filtering does not change the gain therefore is unlikely to cause an opening of the throttle.	DTC for sensors not within the valid range. DTC Position does not match commanded Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.1.2.3 Faulty A/D Conversion	An increased resistance could result in, faulty A/D Conversion which would decrease both VTA's, resulting in an increase in throttle opening, as covered in 2.1.1.1.1.1 Stuck or flipped higher significant bits create an offset to both VTA signals resulting in higher signal voltage on VTA1 closes the throttle. Stuck or flipped lower significant bits create an offset to both VTA	DTC for sensors not within the valid range. DTC Position does not match commanded Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed.

Throttle Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
			signals resulting in lower signal voltage opening the throttle. A stuck bit would be seen other analog sensors such as temperatures, voltages, etc.	Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.1.2.4 Faulty Power	A low voltage monitor inside the ECM that causes a CPU reset and also disables the H-Bridge drive to the motor would detect faulty +12 volts and Vc. Diode protection and multiple regulators mitigate high voltage faults. Multiple VIAs[1] between layers were observed on printed circuit cards.	DTC for sensors not within the valid range. DTC Position does not match commanded Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
	2.1.1.1.3 CPU and Software	2.1.1.1.3.1 Faulty ASIC Hardware	A faulty ASIC would result in a stalled vehicle, except for those covered in 2.1.1.1.2 ECM Input Hardware to A/D.	DTC for sensors not within the valid range. DTC Position does not match commanded Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.1.3.2 Software Error	With the tools utilized during the course of this study, software defects that unilaterally open the throttle or defeat defenses were not found. Extensive software testing and analysis was performed on Toyota 2005 Camry L4 source code using static analysis, logic model testing, recursion testing, and worse case execution timing.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released Engine Turned Off
		2.1.1.1.3.3 Learning Incorrect	A failure of the learning algorithm that could unilaterally open the throttle was not found (see 2.1.1.3.2 Software Error. High VTA1 voltage at ignition key turn on could falsely result in a high learned throttle angle potentially creating a larger than desired throttle command. As described in 2.1.1.1.1. Throttle Position Sensors input, Power and Wiring, the learning algorithm, while not a cause of a failure, compensates for sensor variations, potentially opening the throttle.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released Engine Turned Off
		2.1.1.1.3.4 Faulty Power	A low voltage monitor for +12 volts, and +5 volts inside the ECM that causes a CPU reset and also disables the H-Bridge drive to the motor would detect faulty +12 volts and Vc. Diode protection and multiple regulators mitigate high voltage faults. Multiple VIAs[1] between layers were observed on printed circuit cards.	DTC High current, duty Cycle, or temperature Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal If airflow increases by a large amount after motor disabled, vehicle is shut down
		2.1.1.1.3.5 Faulty Watchdog Timer/Reset	If a Faulty Watchdog Timer/Reset failed “asserted” within one CPU, that specific CPU would reset, the H-Bridge would be disabled; the throttle would close, with no further control of the vehicle. The reset CPU would stop producing the continuous heartbeat output, and this would be sensed and cause a reset of the other CPU.	Engine Turned Off.

[1] Vertical Interconnect Access - a vertical electrical connection between different layers of conductors in printed circuit board.

Throttle Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
			A Faulty Watchdog Timer/Reset failed in the “not asserted” state would require failures in the both the watchdog hardware, and the CPU software to support an opening of the throttle valve. The watchdog software, heartbeat hardware, heartbeat software, and H-Bridge enabling software would all need to fail “operational” within a failed CPU to mask the CPU failure from the system.	
		2.1.1.1.3.6 Faulty Voltage Monitor	If a Faulty Voltage Monitor failed “asserted”, both processors would shut down, the H-Bridge would be disabled; the throttle would close, with no further control of the vehicle. If the reset failed in the "don't assert" state, a second set of failures would be necessary to open the throttle for a UA to occur.	Engine Turned Off.
		2.1.1.1.3.7 Faulty Main/Sub Monitor	If a Faulty Main/SubMonitor failed “asserted”, both processors would shut down, the H-Bridge would be disabled; the throttle would close, with no further control of the vehicle. If the reset failed in the "don't assert" state, a second set of failures would be necessary to open the throttle for a UA to occur.	Engine Turned Off.
	2.1.1.1.4 PWM, Drive and Motor	2.1.1.1.4.1 PWM FET Faulty	Open, shorted, latchup, or resistive failures of any single H-Bridge FET or shorted failure of the on/off FET would be detected by the high current check which would prevent a persistent increase of the throttle. A resistive increase of M+/M- signals would be compensated by an increased duty cycle. Additionally, a shorted failure of the external power on/off FET would also be mitigated by a drive cutoff function and a power cutoff for sensed failures. Latchup is obviated by use of Silicon on Insulator ASICs.	Hardware power disable and DTC for PWM High current, or temperature, DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold. Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.1.4.2 Power Fault to M+/M-	Motor M+ or M- terminal faults to +12 volts or ground of would be detected and mitigated by multiple means. High current and high temperature checks would result in drive cutoff would prevent these postulated faults from persisting.	Hardware power disable and DTC for PWM High current, or temperature, DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold. Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.1.4.3 FET Latch Up	A single H-Bridge FET latched on would be detected by the high current and high temperature checks, which would result in, drive cutoff for an H-Bridge FET latched on. External power on/off FET latches on would be mitigated by the drive cutoff function as well as the power cutoff for sensed failure.	Hardware power disable and DTC for PWM High current, or temperature, DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold. Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.1.4.4 Mechanical	Any mechanical fault would result in motor high current, high temperature, and/or high motor	Hardware power disable and DTC for PWM High current, or temperature,

Throttle Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
		Fault	duty cycle that would be detected by the monitors and result in drive cutoff.	DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold. Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.1.4.5 Coupled Energy	Coupled energy faults would be detected by high current, high temperature, and/or high motor duty cycle checks resulting in drive cutoff. Coupling of energy with sufficient power to activate the motor was not found.	Hardware power disable and DTC for PWM High current, or temperature, DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold. Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.1.4.6 Poor Connection or Wire Damage	High current and high temperature checks would result in drive cutoff function and a power cutoff for sensed failures.	Hardware power disable and DTC for PWM High current, or temperature, DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold. Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
	2.1.1.1.5 Faulty Power		A low voltage monitor inside the ECM that causes a CPU reset and also disables the H-Bridge drive to the motor would detect faulty +12 volts and Vc. Diode protection and multiple regulators mitigate high voltage faults. Multiple VIAs[1] between layers were observed on printed circuit cards.	DTC for sensors not within the valid range. DTC Position does not match commanded Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
2.1.1.2 Throttle Open More Than Commanded	2.1.1.2.1 PWM, Drive and Motor	2.1.1.2.1.1 PWM FET Faulty	Open, shorted, latchup, or resistive failures of any single H-Bridge FET or shorted failure of the on/off FET would be detected by the high current check which would prevent a persistent increase of the throttle. A resistive increase of M+/M- signals would be compensated by an increased duty cycle. Additionally, a shorted failure of the external power on/off FET would also be mitigated by a drive cutoff function and a power cutoff for sensed failures. Latchup is obviated by use of Silicon on Insulator ASICs.	Hardware power disable and DTC for PWM High current, or temperature, DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold. Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4

Throttle Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
				Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.2.1.2 Power Fault to M+/M-	Motor M+ or M- terminal faults to +12 volts or ground of would be detected and mitigated by multiple means. High current and high temperature checks would result in drive cutoff would prevent these postulated faults from persisting.	Hardware power disable and DTC for PWM High current, or temperature, DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold. Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.2.1.3 FET Latch Up	A single H-Bridge FET latched on would be detected by the high current and high temperature checks, which would result in, drive cutoff for an H-Bridge FET latched on. External power on/off FET latches on would be mitigated by the drive cutoff function as well as the power cutoff for sensed failure.	Hardware power disable and DTC for PWM High current, or temperature, DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold. Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.2.1.4 Mechanical Fault	Any mechanical fault would result in motor high current, high temperature, and/or high motor duty cycle that would be detected by the monitors and result in drive cutoff.	Hardware power disable and DTC for PWM High current, or temperature, DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold. Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.2.1.5 Coupled Energy	Coupled energy faults would be detected by high current, high temperature, and/or high motor duty cycle checks resulting in drive cutoff. Coupling of energy with sufficient power to activate the motor was not found.	Hardware power disable and DTC for PWM High current, or temperature, DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold. Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.1.2.1.6 Poor Connection or Wire Damage	High current and high temperature checks would result in drive cutoff function and a power cutoff for sensed failures.	Hardware power disable and DTC for PWM High current, or temperature, DTC when commanded versus measured position do not agree, DTC when PID controlled increases motor duty cycle up to current limit threshold.

Throttle Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
				Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
	2.1.1.2.2 CPU and Software	2.1.1.2.2.1 Software Error	With the tools utilized during the course of this study, software defects that unilaterally open the throttle or defeat defenses were not found. Extensive software testing and analysis was performed on Toyota 2005 Camry L4 source code using static analysis, logic model testing, recursion testing, and worse case execution timing.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released Engine Turned Off
	2.1.1.2.3 Faulty Power		A low voltage monitor inside the ECM that causes a CPU reset and also disables the H-Bridge drive to the motor would detect faulty +12 volts and Vc. Diode protection and multiple regulators mitigate high voltage faults. Multiple VIAs[1] between layers were observed on printed circuit cards.	DTC for sensors not within the valid range. DTC Position does not match commanded Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal

B-2. Pedal Function Fishbone

The Pedal Command Function converts two accelerator pedal position sensors inputs into a desired throttle angle command. The accelerator, pedal along with cruise control, are the only inputs that can command the full range of throttle motion without limit. The pedal assembly consists of the pedal body with two sensors and interfaces to the ECM and related software. Figure B2-1 is the fishbone for the Pedal Function only. Table B2-1 lists the dispositions for each element in the fishbone.

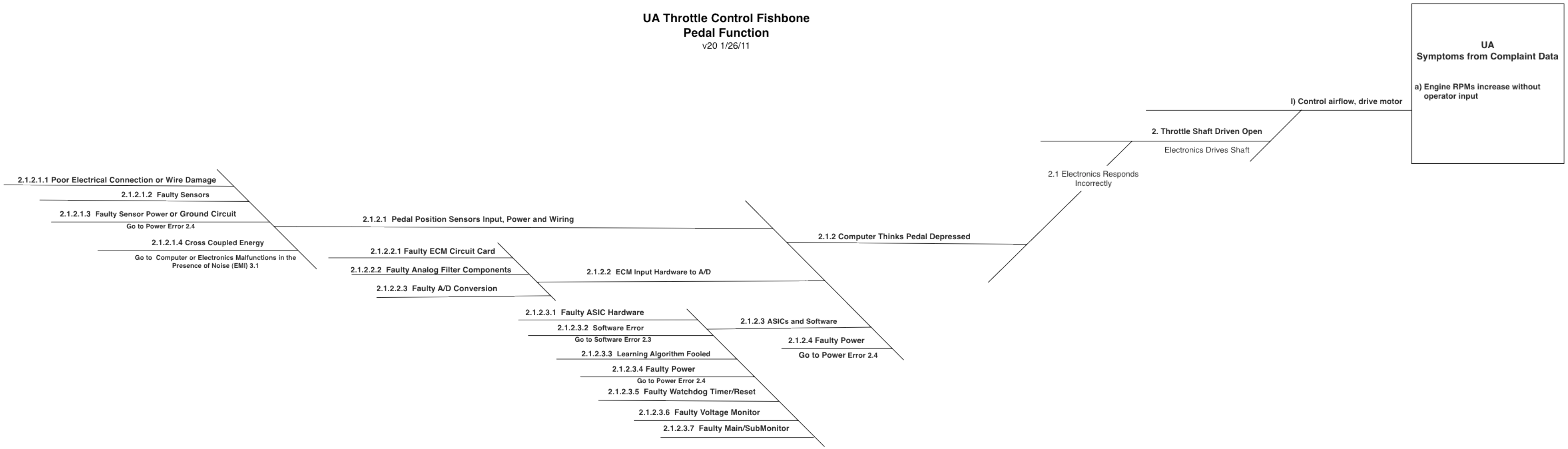

Figure B2-1. Pedal Fishbone Diagram

Table B2-1. Pedal Fishbone Summary of Design Sensitivities with Postulated Faults

Pedal Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
2.1.2 Computer Thinks Pedal Depressed	2.1.2.1 Pedal Position Sensors Input, Power and Wiring	2.1.2.1.1 Poor Electrical Connection or Wire Damage	An increased resistance fault of pedal voltage supply, VCP1 and VCP2 can result in a throttle increase limited to 10 degrees in throttle command. The increased resistance will result in a drop in VPA signals that will be compensated for by the learning algorithm. Removal of the fault will then result in an increase in throttle opening. This sensitivity requires postulated faults in two signals and the condition to be learned then removed. The cause of such a failure would be a poor electrical connection, which would most likely manifest as an increased resistance in the electrical circuit.	DTC for high, low and outside lane. None, if Pedal sensors fail within operational lane DTC Limp Home Mode #1, Throttle control limited to 15 degrees relative opening above idle, by remaining sensor. If neither Pedal Sensor operable then Idle only
			A double series or parallel resistance fault between pedal sensors or sensor to the supply voltage placing VPA1 and VPA2 in their operational lane cannot be detected as a fault and may result in increased throttle opening. This postulated fault requires two independent set of conditions to create UAs in two pedal types. This sensitivity requires postulated faults in two signals which may results in any throttle command even up to full throttle and the condition would be present as long as the fault is present. Either two simultaneous or latent and second faults are required. Series resistance will result in a lower voltage and closing of the throttle or lowering of the learned release position.	Dual Failures within Operational Lane: Engineered Fault in operational lane Valid pedal signal escapes detection, no DTC No mitigation possible for multiple failures that look like a valid pedal signal
		2.1.2.1.2 Faulty Sensors	Potentiometer type: There were no single failure causes found which manifests as a valid command and concurrently (< 0.5sec) impacts both VPA1 & VPA2. High series resistive connections or shorts to +5 volts or ground of VPA1 to VPA2 do not result in an increase in throttle opening. There are dual failures that can open the throttle caused by resistive shorts of VPA1 to VPA2 and a second short between VPA2 and +5 volts or an open on VPA2's return. A second resistive short to ground on VPA1 might result in closing of the throttle or lowering the learned value when the accelerator pedal is released. The dual failures results in opening the throttle as long as resulting voltages remain in the operational lane. A resistive fault between VPA1 & VPA2 (due to tin whiskers) was discovered on a defective pedal with a potentiometer sensor.	DTC for high, low and outside lane. None, if Pedal sensors fail within operational lane DTC Limp Home Mode #1, Throttle control limited to 15 degrees relative opening above idle, by remaining sensor. If neither Pedal Sensor operable then Idle only. (There are particular ignition key cycles and pedal application conditions where the throttle opening may not be limited to 15 degrees after DTC 2121 is detected. These are captured in the "Pedal Resistive Fault Event Sequence Diagram (Figure 6.6.2.3-2).
			Hall Effect: There were no Single failure causes found which manifests as a valid command and concurrently (< 0.5sec) impacts both VPA1 & VPA2. High series resistive connections or shorts to +5 volts or ground of VPA1 to VPA2 do not result in an increase in throttle opening. There are dual failures that can open the throttle caused by resistive shorts of VPA1 to VPA2 and a second short between VPA2 and +5 volts or an open on VPA2's return. A second resistive short to ground on VPA1 might result in closing of the throttle or lowering the learned value when the accelerator pedal is released. The dual failures results in opening the throttle as long as resulting voltages remain in the operational lane. No DC magnetic source was identified near the pedal, which could cause a faulty sensor signals that would last for several seconds or minutes and then disappear. The Earth's magnetic field is orders of magnitude too weak to perturb the sensor signal. Failure of Hall sensor internal circuitry is mitigated be comparison to second sensor.	DTC for high, low and outside lane. None, if Pedal sensors fail within operational lane DTC Limp Home Mode #1, Throttle control limited to 15 degrees relative opening above idle, by remaining sensor. If neither Pedal Sensor operable then Idle only
		2.1.2.1.3 Faulty Sensor Power or Ground Circuit	An increased resistance fault of pedal voltage supply, VCP1 and VCP2 can result in a throttle increase limited to 5 degrees in throttle command, as described in 2.1.2.1.1 Poor Electrical Connection or Wire Damage.	DTC for high, low and outside lane. None, if Pedal sensors fail within operational lane DTC Limp Home Mode #1, Throttle control limited to 15 degrees relative opening above idle, by remaining sensor. If neither Pedal Sensor operable then Idle only
			A double series or parallel resistance fault between pedal sensors or sensor to the supply	Dual Failures within Operational Lane:

Pedal Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
			voltage placing VPA1 and VPA2 in their operational lane cannot be detected as a fault and may result in increased throttle opening, as described in 2.1.2.1.1 Poor Electrical Connection or Wire Damage.	Engineered Fault in operational lane Valid pedal signal escapes detection, no DTC No mitigation possible for multiple failures that look like a valid pedal signal
		2.1.2.1.4 Cross Coupled Energy	Coupling on a single signal sensor lead or the total wire bundle did not result in a throttle opening. Vehicle level EMC testing with current injection in both VPA signals noted an engine rpm increase at various frequencies from 200Hz to 150KHz. At a 500Hz sine wave audio signal aliasing was observed between the pedal input signal and the throttle output. Similarly, component level noise rejection testing noted aliasing at 500Hz on both the VPA signals. See EMI branch 3.1.	DTC for high, low and outside lane. None, if Pedal sensors fail within operational lane DTC Limp Home Mode #1, Throttle control limited to 15 degrees relative opening above idle, by remaining sensor. If neither Pedal Sensor operable then Idle only
	2.1.2.2 ECM Input Hardware to A/D	2.1.2.2.1 Faulty ECM Circuit Card	A double series or parallel resistance fault between pedal sensors or sensor to the supply voltage placing VPA1 and VPA2 in their operational lane cannot be detected as a fault and may result in increased throttle opening, as described in 2.1.2.1.1 Poor Electrical Connection or Wire Damage.	Dual Failures within Operational Lane: Engineered Fault in operational lane Valid pedal signal escapes detection, no DTC No mitigation possible for multiple failures that look like a valid pedal signal
		2.1.2.2.2 Faulty Analog Filter Components	Cracked or damaged passive components could result in an increased series resistance that would decrease both VPA's resulting in a decrease in throttle opening, as covered in 2.1.2.1.1.1 Poor Electrical Connection or Wire Damage. Changes in the cutoff frequency of the filtering does not change the gain therefore is unlikely to cause an opening of the throttle.	Dual Failures within Operational Lane: Engineered Fault in operational lane Valid pedal signal escapes detection, no DTC No mitigation possible for multiple failures that look like a valid pedal signal
		2.1.2.2.3 Faulty A/D Conversion	An increased resistance could result in a faulty A/D Conversion, decreasing both VPA's causing a decrease in throttle opening, as covered in 2.1.2.1.1.1 Stuck or flipped higher significant bits create an offset to both VPA signals resulting in a higher signal voltage on both VPA signals that opens the throttle. Stuck or flipped lower significant bits create an offset to both VPA signals resulting in lower signal voltage that closes the throttle. A stuck bit would be seen other analog sensors such as temperatures, voltages, etc.	Dual Failures within Operational Lane: Engineered Fault in operational lane Valid pedal signal escapes detection, no DTC No mitigation possible for multiple failures that look like a valid pedal signal
	2.1.2.3 ASICs and Software	2.1.2.3.1 Faulty ASIC Hardware	A faulty ASIC would result in a stalled vehicle, except for those covered in 2.1.2.2 ECM Input Hardware to A/D.	DTC for high, low and outside lane. None, if Pedal sensors fail within operational lane DTC Limp Home Mode #1, Throttle control limited to 15 degrees relative opening above idle, by remaining sensor. If neither Pedal Sensor operable then Idle only
		2.1.2.3.2 Software Error	With the tools utilized during the course of this study, software defects that unilaterally open the throttle or defeat defenses were not found. Extensive software testing and analysis was performed on Toyota 2005 Camry L4 source code using static analysis, logic model testing, recursion testing, and worse case execution timing.	None possible, software error opening the throttle would appear normal without watchdog timeout or other errors. Engine Turned Off
		2.1.2.3.3 Learning Algorithm Incorrect	A failure of the learning algorithm that could unilaterally open the throttle was not found (see 2.1.2.3.2 Software Error). As described in 2.1.2.1.3 Faulty Sensors Power pedal voltage supply the learning algorithm, while not a cause of a failure, compensates for sensor variations, increasing the throttle.	DTC for high, low and outside lane. None, if Pedal sensors fail within operational lane DTC Limp Home Mode #1, Throttle control limited to 15 degrees relative opening above idle, by remaining sensor. If neither Pedal Sensor operable then Idle only
		2.1.2.3.4 Faulty Power	A low voltage monitor inside the ECM that causes a CPU reset and also disables the H-Bridge drive to the motor would detect faulty +12 volts and Vc. Diode protection and multiple regulators mitigate high voltage faults. Multiple VIAs[1] between layers were observed on printed circuit cards.	DTC High current, duty Cycle, or temperature Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
		2.1.2.3.5 Faulty	If a Faulty Watchdog Timer/Reset failed "asserted" within one CPU, that specific CPU would	Engine Turned Off

Pedal Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
		Watchdog Timer/Reset	reset, the H-Bridge would be disabled; the throttle would close, with no further control of the vehicle. The reset CPU would stop producing the continuous heartbeat output, and this would be sensed and cause a reset of the other CPU. A Faulty Watchdog Timer/Reset failed in the "not asserted" state would require failures in the both the watchdog hardware, and the CPU software to support an opening of the throttle valve. The watchdog software, heartbeat hardware, heartbeat software, and H-Bridge enabling software would all need to fail "operational" within a failed CPU to mask the CPU failure from the system.	
		2.1.2.3.6 Faulty Voltage Monitor	If a Faulty Voltage Monitor failed "asserted", both processors would shut down, the H-Bridge would be disabled; the throttle would close, with no further control of the vehicle. If the reset failed in the "don't assert" state, a second failure would be necessary for a UA to occur.	Engine Turned Off
		2.1.2.3.7 Faulty Main/SubMonitor	If a Faulty Main/SubMonitor failed "asserted", both processors would shut down, the H-Bridge would be disabled; the throttle would close, with no further control of the vehicle. If the reset failed in the "don't assert" state, a second failure would be necessary for a UA to occur.	Engine Turned Off
	2.1.2.4 Faulty Power		A low voltage monitor inside the ECM that causes a CPU reset and also disables the H-Bridge drive to the motor would detect faulty +12 volts and Vc. Diode protection and multiple regulators mitigate high voltage faults. Multiple VIAs[1] between layers were observed on printed circuit cards.	DTC High current, duty Cycle, or temperature Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal

B-3. Cruise Control Function

Cruise Control receives inputs from the cruise control switch along with transmission gear selector, brake engagement, and vehicle speed signals to maintain and modulate vehicle speed without accelerator pedal inputs. It also disengages cruise control when commanded. Figure B3-1 is the fishbone for the Cruise Control Function. Table B3-1 lists the dispositions for each element in the fishbone.

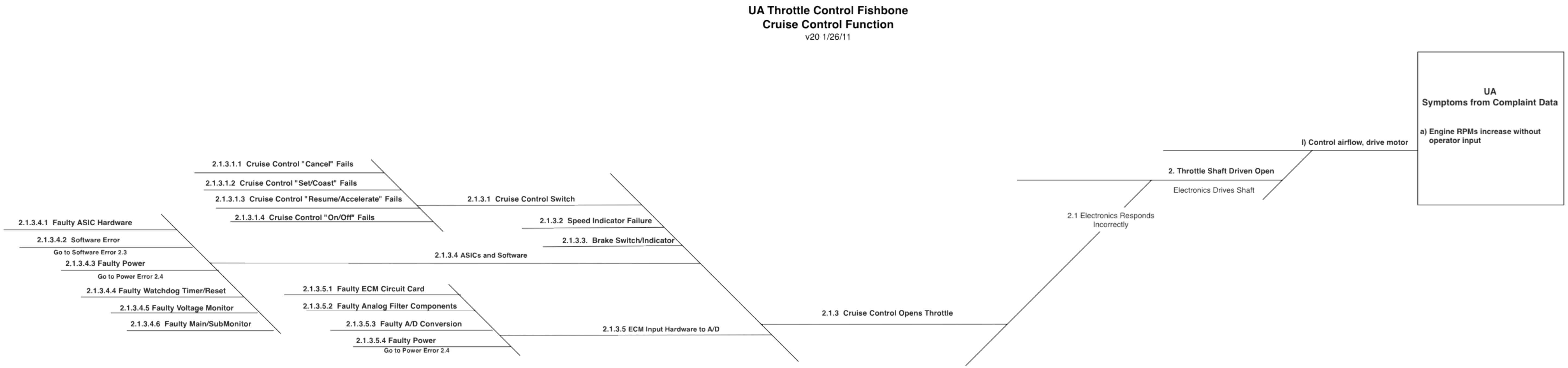

Figure B3-1. Cruise Control Fishbone Diagram

Table B3-1. Cruise Control Fishbone Summary of Design Sensitivities with Postulated Faults

Cruise Control Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
2.1.3 Cruise Control Opens Throttle	2.1.3.1 Cruise Control Switch	2.1.3.1.1 Cruise Control "Cancel" Fails	There are multiple mitigations and protections in place to protect against a failed Cruise Control "Cancel" failures. Normal switch position is "OFF.	Specific ordering for activation, Short to ground is "OFF" Driver can cancel, Brake Switch, or 9 MPH slow down cancels Cruise, or shift to neutral
		2.1.3.1.2 Cruise Control "Set/Coast" Fails	There are multiple mitigations and protections in place to protect against a failed Cruise Control "Set/Cancel" failures. Normal switch position is "OFF". Engaging the set switch for longer than 0.6 seconds results in coast and a decrease the vehicle speed of the vehicle.	Specific ordering for activation, Short to ground is "OFF" Driver can activate, Brake Switch, or 9 MPH slow down cancels Cruise, or cancel cruise, or shift to neutral
		2.1.3.1.3 Cruise Control "Resume/Accelerate" Fails	A resistive short of the cruise control signal wire to ground of the Cruise Control "Resume/Accelerate" with the cruise control engaged, will result in the vehicle accelerating to the maximum speed threshold of the system. Application of the brake pedal will cancel cruise control.	Specific ordering for activation, Short to ground is "OFF" Driver can cancel, Brake Switch, or 9 MPH slow down cancels Cruise, or shift to neutral
		2.1.3.1.4 Cruise Control "On/Off" Fails	There are multiple mitigations and protections in place to protect against a failed Cruise Control "Cancel" failures. Normal switch position is "OFF.	Specific ordering for activation, Short to ground is "OFF" Driver can cancel, Brake Switch, or 9 MPH slow down cancels Cruise, or shift to neutral
	2.1.3.2 Speed Indicator Failure		There are multiple mitigations and protections in place If a faulty wheel speed signal indicates a slower speed than the actual vehicle speed causing an increase in throttle to maintain set speed. Acceleration is limited to 0.6 g. The operator has 5 methods to cancel cruise.	Sensor ignored, Cruise Control Cancel at 9 MPH reduction Driver can cancel, Brake Switch, or 9 MPH slow down cancels Cruise or shift to neutral
	2.1.3.3. Brake Switch/Indicator		Cruise control remains activated and functioning even when brake pedal applications are induced with the loss of brake switch plunger or both normally open and normally closed brake switch contacts. Set speed is maintained until enough brake force is applied to decrease vehicle speed by approximately 9 mph or below the 25 mph threshold of operation causing the system to fully disengage. No DTC will be set.	Car accelerates at 0.06g to maintain set speed. Cancel or Off necessary to disable Cruise Control Driver can cancel, Brake Switch, or 9 MPH slow down cancels Cruise, or shift to neutral
	2.1.3.4 ASICs and Software	2.1.3.4.1 Faulty ASIC Hardware	A faulty ASIC would result in a stalled vehicle, except for those covered in 2.1.2.2 ECM Input Hardware to A/D.	Specific ordering for activation, Short to ground is "OFF" Driver can cancel, Brake Switch, or 9 MPH slow down cancels Cruise or shift to neutral Engine Turned Off #6

Cruise Control Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
		2.1.3.4.2 Software Error	With the tools utilized during the course of this study, software defects that unilaterally open the throttle or defeat defenses were not found. Extensive software testing and analysis was performed on Toyota 2005 Camry L4 source code using static analysis, logic model testing, recursion testing, and worse case execution timing.	None possible, software error opening the throttle would appear normal without watchdog timeout or other errors. Driver can cancel, Brake Switch, or 9 MPH slow down cancels Cruise or shift to neutral Engine Turned Off
		2.1.3.4.3 Faulty Power	A low voltage monitor inside the ECM that causes a CPU reset and also disables the H-Bridge drive to the motor would detect faulty +12 volts and Vc. Diode protection and multiple regulators mitigate high voltage faults. Multiple VIAs[1] between layers were observed on printed circuit cards.	DTC High current, duty Cycle, or temperature Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
		2.1.3.4.4 Faulty Watchdog Timer/Reset	If a Faulty Watchdog Timer/Reset failed “asserted” within one CPU, that specific CPU would reset, the H-Bridge would be disabled; the throttle would close, with no further control of the vehicle. The reset CPU would stop producing the continuous heartbeat output, and this would be sensed and cause a reset of the other CPU. A Faulty Watchdog Timer/Reset failed in the “not asserted” state would require failures in the both the watchdog hardware, and the CPU software to support an opening of the throttle valve. The watchdog software, heartbeat hardware, heartbeat software, and H-Bridge enabling software would all need to fail “operational” within a failed CPU to mask the CPU failure from the system.	Engine Turned Off
		2.1.3.4.6 Faulty Voltage Monitor	If a Faulty Voltage Monitor failed “asserted”, both processors would shut down, the H-Bridge would be disabled; the throttle would close, with no further control of the vehicle. If the reset failed in the "don't assert" state, a second failure would be necessary for a UA to occur.	Engine Turned Off.
		2.1.3.4.5 Faulty Main/SubMonitor	If a Faulty Main/SubMonitor failed “asserted”, both processors would shut down, the H-Bridge would be disabled; the throttle would close, with no further control of the vehicle. If the reset failed in the "don't assert" state, a second failure would be necessary for a UA to occur.	Engine Turned Off.
	2.1.3.5 ECM Input Hardware to A/D	2.1.3.5.1 Faulty ECM Circuit Card	There are multiple mitigations and protections in place to protect against a failed Cruise Control "Cancel" failures. Normal switch position is "OFF.	Specific ordering for activation, Short to ground is "OFF" Driver can cancel, Brake Switch, or 9 MPH slow down cancels Cruise, e, or shift to neutral Engine Turned Off #6

Cruise Control Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
		2.1.3.5.2 Faulty Analog Filter Components	There are multiple mitigations and protections in place to protect against a failed Cruise Control "Cancel" failures. Normal switch position is "OFF.	Specific ordering for activation, Short to ground is "OFF" Driver can cancel, Brake Switch, or 9 MPH slow down cancels Cruise, e, or shift to neutral. Engine Turned Off #6
		2.1.3.5.3 Faulty A/D Conversion	There are multiple mitigations and protections in place to protect against a failed Cruise Control "Cancel" failures. Normal switch position is "OFF.	Specific ordering for activation, Short to ground is "OFF" Driver can cancel, Brake Switch, or 9 MPH slow down cancels Cruise, e, or shift to neutral Engine Turned Off #6
		2.1.3.5.4 Faulty Power	A low voltage monitor inside the ECM that causes a CPU reset and also disables the H-Bridge drive to the motor would detect faulty +12 volts and Vc. Diode protection and multiple regulators mitigate high voltage faults. Multiple VIAs1 between layers were observed on printed circuit cards.	DTC High current, duty Cycle, or temperature Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal

B-4. Idle Speed Control Function

The Idle Speed Control Function is one of the more complex functions in the system. Engine rpm, transmission gear selection, air condition engagement, electric load, engine temperature, coolant temperature, vehicle speed, and brake switch engagement are all used to modulate the throttle to manage idle speed control. Figure B4-1 is the fishbone for the Idle Speed Control. Table B4-1 lists the dispositions for each element in the fishbone.

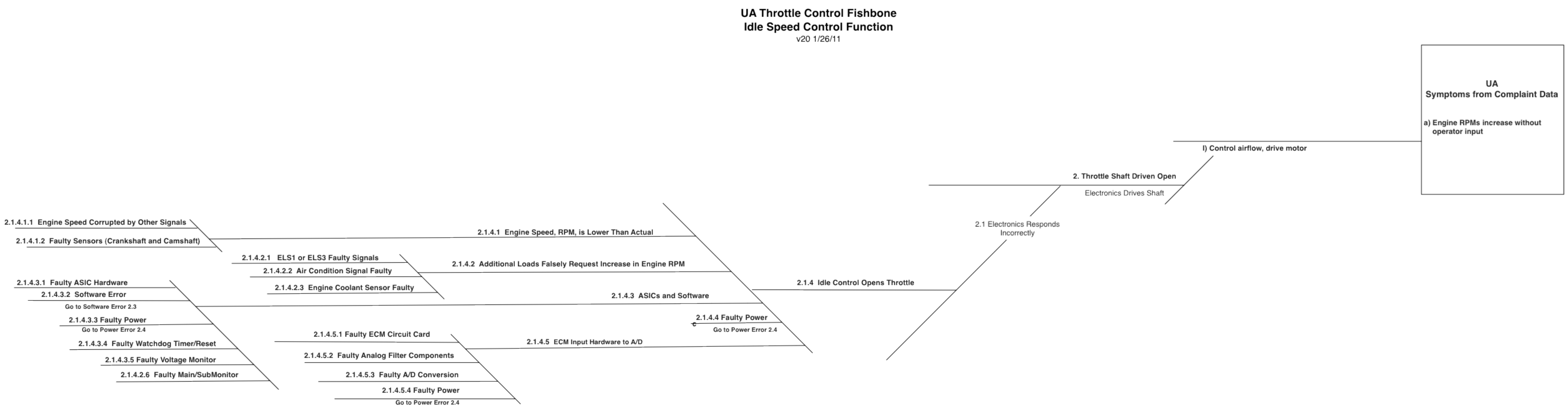

Figure B4-1. Idle Speed Control Fishbone Diagram

Table B4-1. Idle Speed Control Fishbone Summary of Design Sensitivities with Postulated Faults

Idle Speed Control Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
2.1.4 Idle Speed Control Opens Throttle	2.1.4.1 Engine Speed, RPM, signal is Lower Than Actual	2.1.4.1.1 Engine Speed signal Corrupted by Other Signals	False indication of low engine speed, calculated from crankshaft and camshaft signals, may result in idle speed control creating rpm increase to achieve the target rpm. Any corruption of the crankshaft and camshaft signals that fails to maintain the proper timing relative to the actual engine speed will stall the engine. No signal was identified that mimics the crankshaft signal and can maintain the proper timing relative to the actual engine rotation. Testing of the crankshaft signal indicated no sensitivity to offset voltages. A DC bias or offset could corrupt the zero crossing detecting circuit resulting in a change to the signal duty cycle but not the frequency.	Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.4.1.2 Faulty Sensors (Crankshaft and Camshaft)	False indication of low engine speed, calculated from crankshaft and camshaft signals, may result in idle speed control creating rpm increase. No fault was identified in the crankshaft/camshaft sensors that would result in a lower reported engine speed without causing an engine stall.	Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
	2.1.4.2 Additional Loads Falsely Request Increase in Engine RPM	2.1.4.2.1 Electric Load Signal 1 or Electric Load Signal 3 Faulty Signals	Fault testing indicated that the throttle increase demand from Electric Load Signal 1 and Electric Load Signal 3 was negligible.	Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.4.2.2 Air Conditioner Compressor On Indication Signal Faulty	Fault testing indicated that the throttle increase demand from the air condition compressor on indication signal resulting in a 200 rpm increase and was not considered a significant engine rpm increase.	Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.4.2.3 Engine Coolant Sensor Faulty	A failure limits the throttle to openings to 5 degrees between normal sensor values and DTC limit. Testing indicated that an increase in resistance of the electrical connection of the engine coolant sensor will result in increasing the idle engine speed by up to 2000 rpm. A resistance increase will not trip a DTC until roughly 149Kohms.	Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
	2.1.4.3 ASICs and Software	2.1.4.3.1 Faulty ASIC Hardware	A faulty ASIC would result in a stalled vehicle, except for those covered in 2.1.2.2 ECM Input Hardware to A/D.	Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.4.3.2 Software Error	With the tools utilized during the course of this study, software defects that unilaterally open the throttle or defeat defenses were not found. Extensive software testing and analysis was performed on Toyota 2005 Camry L4 source code using static analysis, logic model testing, recursion testing, and worse case execution timing.	None possible, software error opening the throttle would appear normal without watchdog timeout or other errors. Driver can cancel, Brake Switch, or 9 MPH slow down cancels Cruise or shift to neutral Engine Turned Off

Idle Speed Control Function Fishbone Disposition			Description and Disposition	Detection & System Level Mitigations
		2.1.4.3.3 Faulty Power	A low voltage monitor inside the ECM that causes a CPU reset and also disables the H-Bridge drive to the motor would detect faulty +12 volts and Vc. Diode protection and multiple regulators mitigate high voltage faults. Multiple VIAs[1] between layers were observed on printed circuit cards.	DTC High current, duty Cycle, or temperature Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
		2.1.4.3.4 Faulty Watchdog Timer/Reset	If a Faulty Watchdog Timer/Reset failed "asserted" within one CPU, that specific CPU would reset, the H-Bridge would be disabled; the throttle would close, with no further control of the vehicle. The reset CPU would stop producing the continuous heartbeat output, and this would be sensed and cause a reset of the other CPU. A Faulty Watchdog Timer/Reset failed in the "not asserted" state would require failures in the both the watchdog hardware, and the CPU software to support an opening of the throttle valve. The watchdog software, heartbeat hardware, heartbeat software, and H-Bridge enabling software would all need to fail "operational" within a failed CPU to mask the CPU failure from the system.	Engine Turned Off
		2.1.4.3.5 Faulty Voltage Monitor	If a Faulty Voltage Monitor failed "asserted", both processors would shut down, the H-Bridge would be disabled; the throttle would close, with no further control of the vehicle. If the reset failed in the "don't assert" state, a second failure would be necessary for a UA to occur.	Engine Turned Off
		2.1.4.3.6 Faulty Main/SubMonitor	If a Faulty Main/SubMonitor failed "asserted", both processors would shut down, the H-Bridge would be disabled; the throttle would close, with no further control of the vehicle. If the reset failed in the "don't assert" state, a second failure would be necessary for a UA to occur.	Engine Turned Off.
	2.1.4.5 ECM Input Hardware to A/D	2.1.4.5.1 Faulty ECM Circuit Card	A faulty ECM Circuit Card could mimic the symptoms of a faulty engine coolant sensor, limits throttle to openings from less than 3 degrees to 5 degrees. No other fault was identified in the idle speed control inputs that could result in an UA.	Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.4.5.2 Faulty Analog Filter Components	Faulty analog filter components could mimic the symptoms of a faulty engine coolant sensor, limits throttle to openings from less than 3 degrees to 5 degrees. No other fault was identified in the idle speed control inputs that could result in an UA.	Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.4.5.3 Faulty A/D Conversion	Faulty A/D conversion could mimic the symptoms of a faulty engine coolant sensor, limits throttle to openings from less than 3 degrees to 5 degrees. No other fault was identified in the idle speed control inputs that could result in an UA.	Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released
		2.1.4.5.4 Faulty Power	A low voltage monitor inside the ECM that causes a CPU reset and also disables the H-Bridge drive to the motor would detect faulty +12 volts and Vc. Diode protection and multiple regulators mitigate high voltage faults. Multiple VIAs[1] between layers were observed on printed circuit cards.	DTC High current, duty Cycle, or temperature Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal

B-5. Transmission Shifting and Vehicle Stability Control Function

Transmission Shifting utilizes engine rpm and transmission gear selection signals to modulate the throttle to smoothly shift from one gear to another. This function also controls the torque converter lock up to reduce shift shock. Vehicle Stability Control (VSC) receives a vehicle speed signal input to adjust throttle valve angle to help maintain traction. Prior to MY 2007, the VSC could only reduce throttle command. Figure B5-1 is the fishbone for the Transmission Shifting and VSC Function only. Table B5-1 lists the dispositions for each element in the fishbone.

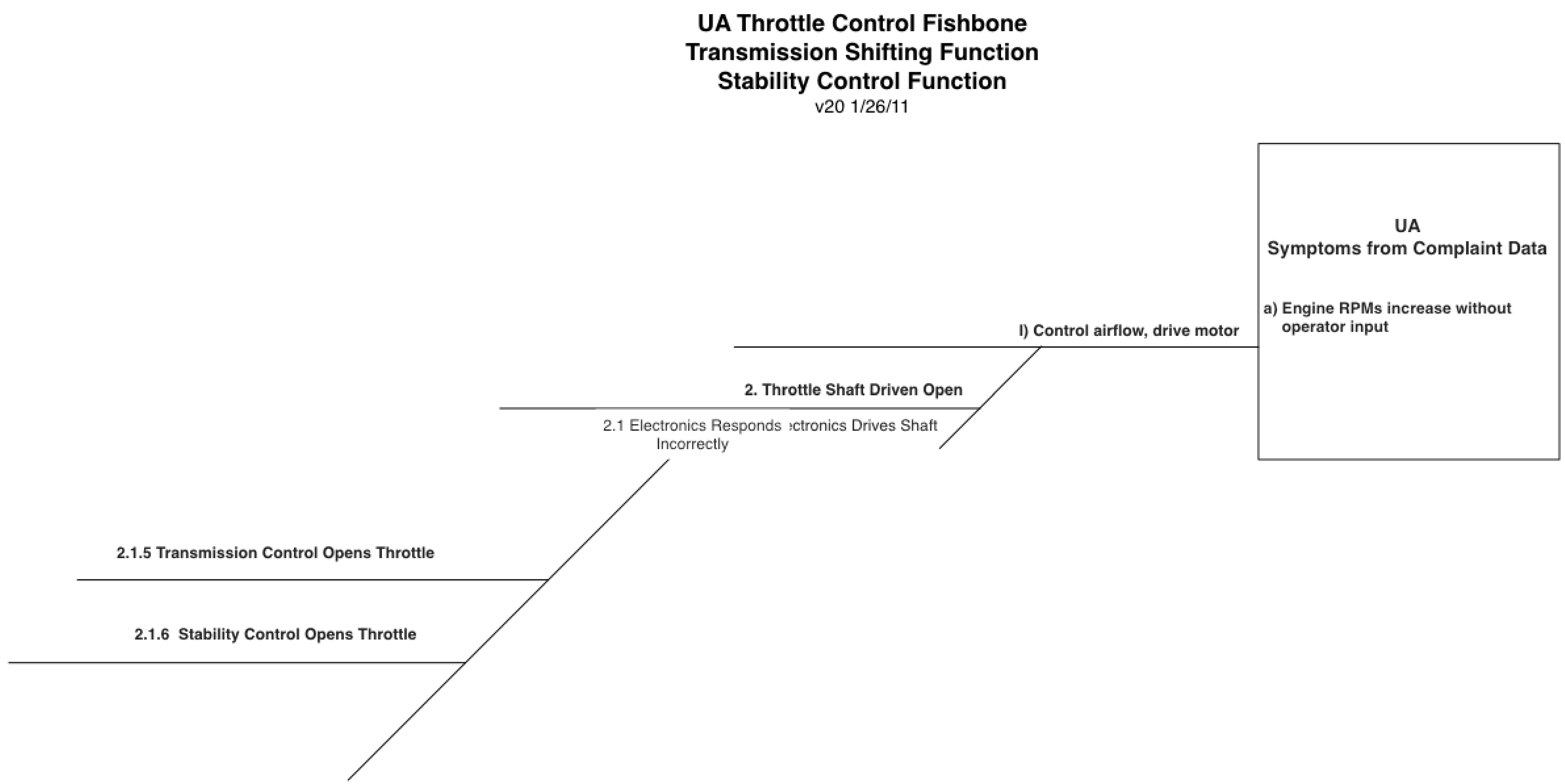

Figure B5-1. Transmission Shifting and Stability Control Fishbone Diagram

Table B5-1. Transmission Shifting and Vehicle Stability Control Fishbone Summary of Design Sensitivities with Postulated Faults

Transmission Control & VSC		Disposition	Detection & System Level Mitigations
2.1.5 Transmission Control Opens Throttle		Failure is limited to throttle openings to 5 degrees.	DTC results in selection up one gear.
2.1.6 Stability Control Opens Throttle		MY 2005 Camry and earlier cannot increase throttle opening. MY 2007-2010 were not studied.	

B-6. Power Fishbone

The power supply ASIC configuration includes [redacted] associated with this ASIC, and the [redacted] to the Main CPU. The Sub-CPU operates from [redacted]. Figure B6-1 is the fishbone for the Power only with those elements that have been identified as design sensitivities with postulated faults denoted by a red square. Table B6-1 lists the dispositions for each element in the fishbone and those design sensitivities with postulated faults are highlighted in yellow.

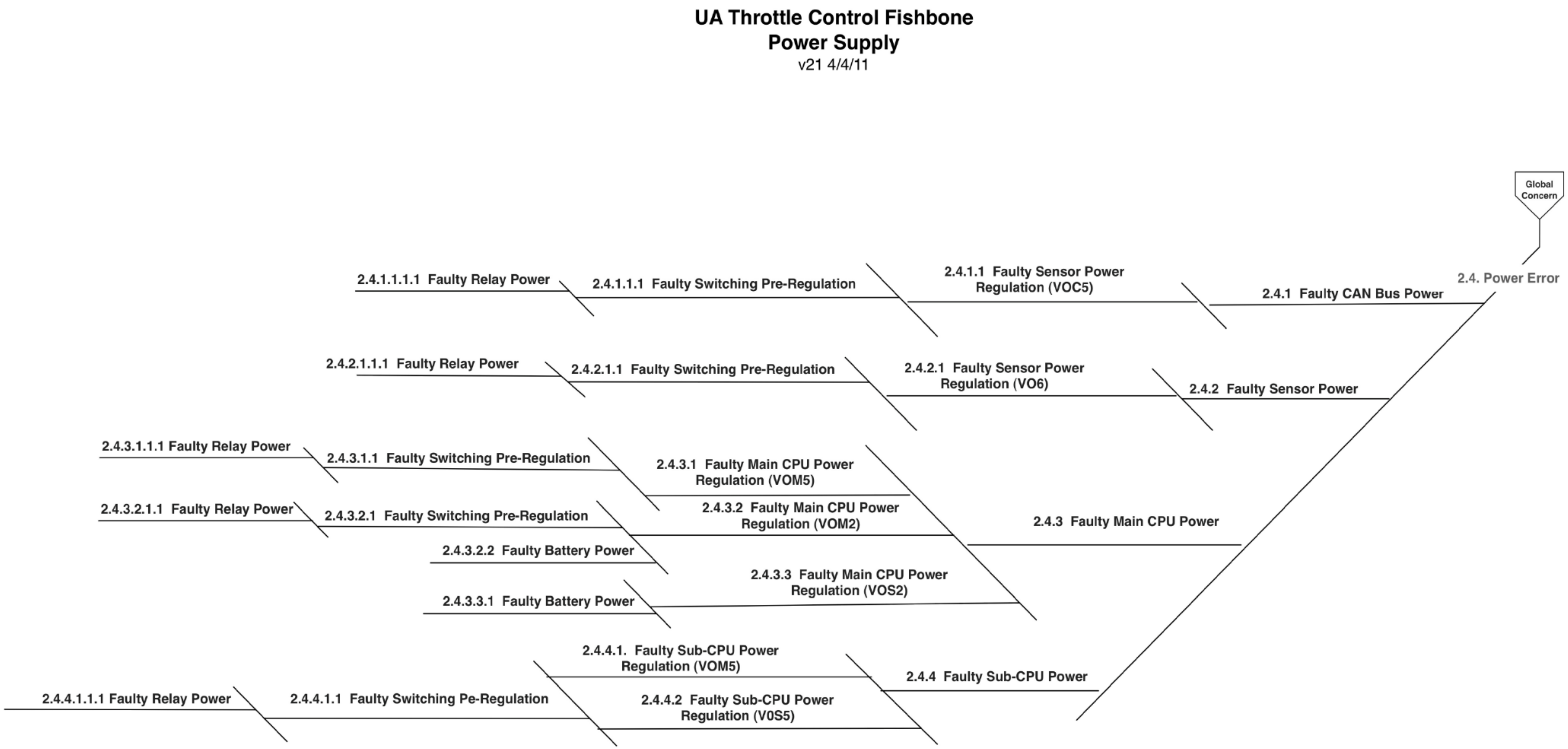

Figure B6-1. Power Fishbone Diagram

Table B6-1. Power Fishbone Summary of Design Sensitivities with Postulated Faults

Power				**Disposition**	**Detection & System Level Mitigations**
2.4.1 Faulty CAN Bus Power	2.4.1.1 Faulty Sensor Power Regulation (VOC5)	2.4.1.1.1 Faulty Switching Pre-Regulation	2.4.1.1.1.1 Faulty Relay Power	A failure of CAN Bus Power interface is limited to the VSC in MY04 & 05 which can only reduce throttle openings. Late MY vehicles (2007 and newer) include other CAN bus interfaces including the Combination Meter, Accessory Gateway, A/C Amplifier, Airbag System, Main Body ECU, and Certification ECU which do not affect engine speed.	Cannot open throttle
2.4.2 Faulty Sensor Power	2.4.2.1 Faulty Sensor Power Regulation (VO6)	2.4.2.1.1 Faulty Switching Pre-Regulation	2.4.2.1.1.1 Faulty Relay Power	[redacted] Throttle valve chatter was observed when the Throttle sensor signal line was shorted to +12v, to M+ or M-, but the chatter was not sustained.	Engine Turned Off
2.4.3 Faulty Main CPU Power	2.4.3.1 Faulty Main CPU Power Regulation (VOM5)	2.4.3.1.1 Faulty Switching Pre-Regulation	2.4.3.1.1.1 Faulty Relay Power	Overloading VOM5 (Vc) results in an engine stall due to foldback current limiting at approximately 520 mA into a short circuit. An overvoltage caused by a short to +12v will cause catastrophic failure of the CPUs. [redacted] is main power for both the main and sub-CPUs, and also is the supply voltage for the throttle and pedal position sensors and the air flow mass sensor.	Engine Turned Off
	2.4.3.2 Faulty Main CPU Power Regulation (VOM2)	2.4.3.2.1 Faulty Switching Pre-Regulation	2.4.3.2.1.1 Faulty Relay Power	Failure of VOM2 would cause a main CPU watchdog timeout resulting in a power reset.	Engine Turned Off
		2.4.3.2.2 Faulty Battery Power		Overvoltage failure would cause a catastrophic failure of the Main CPU. Battery power to this regulator provides memory keep alive power while the ignition/engine is off.	Engine Turned Off
	2.4.3.3 Faulty Main CPU Power Regulation (VOS2)	2.4.3.3.1 Faulty Battery Power		Failure of VOS2 would cause a main CPU watchdog timeout resulting in a power reset. Overvoltage failure would cause a catastrophic failure of the Main CPU. Battery power to this regulator provides memory keep alive power while the ignition/engine is off.	Engine Turned Off

Power				Disposition	Detection & System Level Mitigations
2.4.4 Faulty Sub-CPU Power	2.4.4.1. Faulty Sub-CPU Power (VOM5)	2.4.4.1.1 Faulty Switching Per-Regulation	2.4.4.1.1.1 Faulty Relay Power	[redacted]	Engine Turned Off
	2.4.4.2 Faulty Sub-CPU Power Regulation (V0S5)	2.4.4.1.1 Faulty Switching Per-Regulation	2.4.4.1.1.1 Faulty Relay Power	[redacted]	Engine Turned Off

B-7. Software Error

The throttle control system utilizes software to mimic a mechanical system while providing additional features. The software contains learning algorithms to recalibrate sensor inputs as they vary over life or are influenced by environmental effects. These learning algorithms provide constant and repeatable operating characteristics for the vehicle. Learning algorithms are used in the accelerator pedal section to adjust for the equivalent of play or cable slack present in a mechanical system, idle speed control learns the throttle angle necessary to control engine rpm to the target idle speed considering engine environmental and load conditions, and the throttle control loop learns the sensed fully closed angle at engine start. The software also contains fault detection logic to isolate failed components and respond with an appropriate fail-safe mode that protects the vehicle from unwanted throttle opening. Figure B7-1 is the fishbone for the Software Error only. Table B7-1 lists the dispositions for each element in the fishbone.

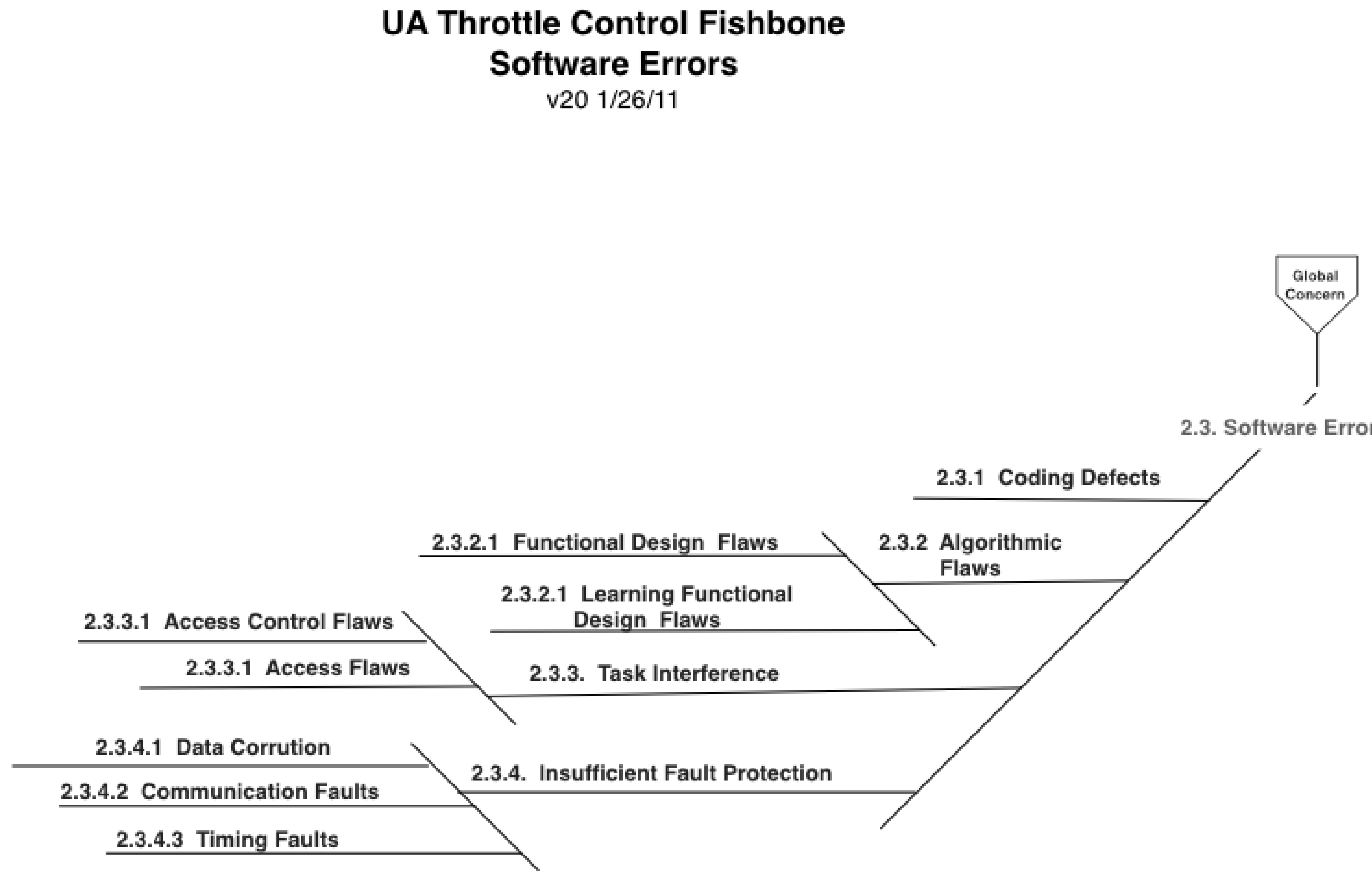

Figure B7-1. Software Error Fishbone Diagram

Table B7-1. Software Error Fishbone Summary of Design Sensitivities with Postulated Faults

2.3. Software		**Disposition**	**Detection & System Level Mitigations**
2.3.1 Coding Defects		Major coding defects that cause the entire system to fail will be detected by the hardware as a watchdog timer reset. This will cause a reset and restart of the two processors. Minor coding defects that affect a partial functional failure of the system will be detected as a mismatch of the relationship between sensors, a mismatch between stored values, or an out-of-bounds value. These will cause one or a combination of: a DTC to be issued, an entry into a failsafe condition, the use of a default operational value. Generally, the precise impact of a coding defect on system functionality cannot accurately be predicted.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released Engine Turned Off.
2.3.2 Algorithmic Flaws	2.3.2.1 Functional Design Flaws	Major functional design flaws that cause the entire system to fail will be detected by the hardware as a Watch Dog timer reset. This normally causes a reset of the two processors. Minor functional design flaws that affect a partial functional failure of the system can be detected as a mismatch of the relationship between sensors, a mismatch between stored values, or an out-of-bounds value. These will cause one or a combination of: a DTC to be issued, an entry into a failsafe condition, the use of a default operational value.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released Engine Turned Off.
	2.3.2.2 Learning Functional Design Flaws	Learning Functional Design Flaws are normally protected in the same manner as 2.3.2.1 Functional Design Flaws. Also, the learned fully-closed throttle position and fully-released pedal position are normally prevented from learning an incorrect value by incorporating the throttle diagnostic failsafe flags as well as using a smoothing function to filter out any spikes in sensor data.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released Engine Turned Off.
2.3.3. Task Interference	2.3.3.1 Access Control Flaws	Shared data requires access control such that data is written and read correctly. For the MY 2005 Camry software, preventing interruptions during any read or write of shared data implements this access control for some, but not all, instances of access. Access control flaws can be detected as a mismatch of the relationship between sensors, a mismatch between stored values, or an out-of-bounds value. These will then cause one or a combination of: a DTC to be issued, an entry into a failsafe condition, the use of a default operational value.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released Engine Turned Off.
	2.3.3.2 Access Flaws	Access flaws, where data is read from the wrong variable, or written to the wrong variable, are not detected in the software or the CPU hardware.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released Engine Turned Off.

2.3. Software		Disposition	Detection & System Level Mitigations
2.3.4. Insufficient Fault Protection	2.3.4.1 Data Corruption	In the MY 2005 Camry software, data mirroring was implemented to detect access flaws. Data corruption may occur when an input buffer is filled beyond its designed size, when the CPU stack extends beyond the depth expected, or when a hardware memory error occurs. When written, data was stored a second time as a complemented value. When read, the two values were checked to be correct. If they did not check, a default value was used.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released Engine Turned Off.
	2.3.4.2 Communication Faults	Two communication paths were studied between the main CPU and the sub CPU: the watchdog heartbeat and the serial data exchange. The watchdog heartbeat is sent from the sub CPU to the main CPU, and from the main CPU to the power control and reset hardware. The heartbeat is a continuous pulse stream. Any interruption of this pulse stream results in the reset and restart of the CPUs. No check or retry is available on the serial data exchange. The data is updated on the next processing cycle, and any errors are detected as a mismatch of the relationship between sensors, a mismatch between stored values, or an out-of-bounds value.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal Idle Mode Fuel Cut, #4 Fuel Cut at 2500 rpm when accelerator pedal released Engine Turned Off.
	2.3.4.3 Timing Faults	A Watchdog Timer/Reset is implemented to detect timing errors. If a Faulty Watchdog Timer/Reset failed “asserted” within one CPU, that specific CPU would reset, the H-Bridge would be disabled; the throttle would close, with no further control of the vehicle. The reset CPU would stop producing the continuous heartbeat output, and this would be sensed and cause a reset of the other CPU. A Faulty Watchdog Timer/Reset failed in the “not asserted” state would require failures in the both the watchdog hardware, and the CPU software to support an opening of the throttle valve. The watchdog software, heartbeat hardware, heartbeat software, and H-Bridge enabling software would all need to fail “operational” within a failed CPU to mask the CPU failure from the system.	Engine Turned Off.

B-8. Environmental Effects Fishbone

Electromagnetic Interference (EMI) can affect electronics in unexpected ways and may not leave physical evidence to guide troubling shooting of unwanted effects. Because of this non-degrading momentary condition, EMI is often postulated as a cause for the UAs described in the complaint data. Comprehensive EMC testing, including radiated susceptibility, conducted transient emissions and conducted transient, and audio and radio frequency susceptibility was performed in support of the investigative process. Six Toyota Camry VOQ report vehicles provided by NHTSA (a 2002 XLE V6, a 2003 XLE L4, a 2004 XLE V6, a 2004 L4, a 2007 XLE V6, and a 2007 L4) were utilized in the EMI testing. Figure B8-1 is the fishbone for the Environmental Effects only. Table B8-1 lists the dispositions for each element in the fishbone. Two additional elements, 3.4 Mechanical Vibration and 3.5 Thermal, were not analyzed or tested, but faults typically induced by these effects are covered in other the Throttle, Pedal, and Power Function fishbones.

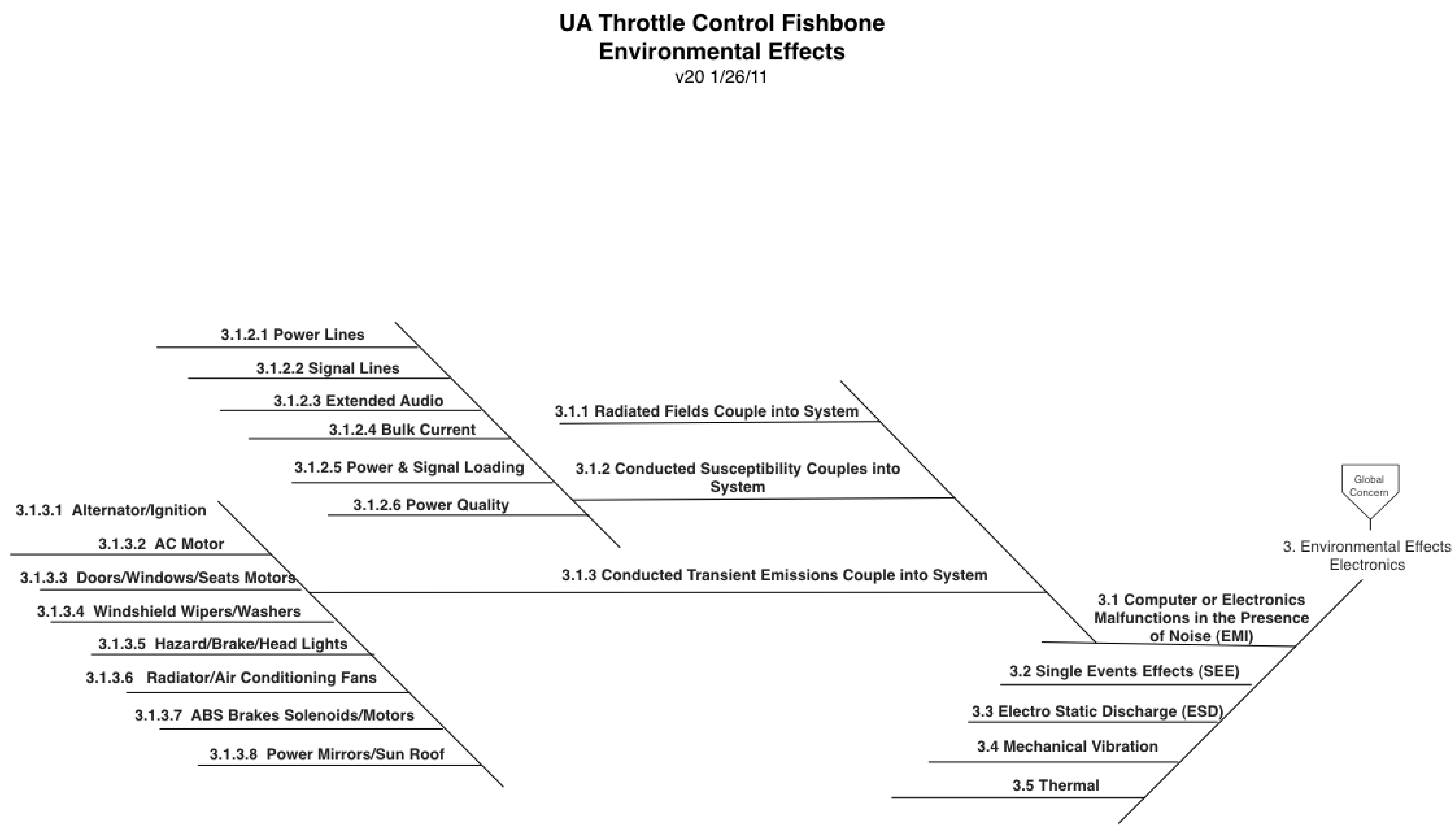

Figure B8-1. Environmental Effects Fishbone Diagram

Table B8-1. Environmental Effects Fishbone Summary of Design Sensitivities with Postulated Faults

Environmental			Disposition	System Level Mitigations
3.1 Computer or Electronics Malfunctions in the Presence of Noise (EMI)	3.1.1 Radiated Fields Couple into System		Radiated susceptibility testing subjected the vehicles under test to RF fields in excess of certification and Toyota acceptance levels. Effects ranged from setting of DTCs, dashboard lights changing state, engine speed reducing, or the engine stalling.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
	3.1.2 Conducted Susceptibility Couples into System	3.1.2.1 Power Lines	No occurrences of unintended or uncommanded acceleration were observed.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
		3.1.2.2 Signal Lines	No occurrences of unintended or uncommanded acceleration were observed. Some disruption on the Cam and Crankshaft signals and some engine stalls were observed.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
		3.1.2.3 Extended Audio	Engine speed increased in response to the presence of a large conducted audio frequency signal, injected in differential mode, simultaneously onto both accelerator pedal sensor signal lines using capacitive coupling. The large magnitude of this signal was injected onto the two wires pulled out of a six-wire harness bundle and thus isolated and injected the noise in a fashion that would not be encountered during normal driving operations	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
		3.1.2.4 Bulk Current	No occurrences of unintended or uncommanded acceleration were observed. Some rpm increase was observed when signals were applied to both pedal signal lines, both signal and voltage supply lines together with no latch-up.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
		3.1.2.5 Power & Signal Loading	No occurrences of unintended or uncommanded acceleration were observed. Some engine stalls were observed.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
		3.1.2.6 Power Quality	No occurrences of unintended or uncommanded acceleration were observed. Some rpm increase coincident with transition to "limp mode" and some engine stalls were observed.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
	3.1.3 Conducted Transient Emissions Couple into System	3.1.3.1 Alternator/Ignition	No significant source/victim transient vulnerabilities were observed. Some coupling was observed from the ignition noise to ECM +5V, VPA1, VTA1. The onboard coupling to throttle control signals from these sources is much less than the levels imposed during conducted susceptibility testing. There is a factor of at least 10 margins between applied test levels and measured noise coupling.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
		3.1.3.2 AC Motor Blower	No significant source/victim transient vulnerabilities were observed. Small transients on VPA1, VTA1, cruise, crank, Cam, MAF, O2, brake signals were observed. The onboard coupling to throttle control signals from these sources is much less than the levels imposed during conducted susceptibility testing. There is a factor of at least 10 margins between applied test levels and measured noise coupling.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
		3.1.3.3 Doors/Windows/Seats Motors	No significant source/victim transient vulnerabilities were observed. Small coupling from door locks to +5V, VPA1, VTA1 Cruise control signal, cam sensor, air flow, O2, brake input. Slight window actuator coupling to +5V, cruise control signal. Seat motor spike on the brake signal. The onboard coupling to throttle control signals from these sources is much less than the levels imposed during conducted susceptibility testing. There is a factor of at least 10 margins between applied test levels and measured noise coupling.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal

Environmental			Disposition	System Level Mitigations
		3.1.3.4 Windshield Wipers/Washers	No significant source/victim transient vulnerabilities were observed. The onboard coupling to throttle control signals from these sources is much less than the levels imposed during conducted susceptibility testing There is a factor of at least 10 margin between applied test levels and measured noise coupling.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
		3.1.3.5 Hazard/Brake/Head Lights	No significant source/victim transient vulnerabilities were observed. The onboard coupling to throttle control signals from these sources is much less than the levels imposed during conducted susceptibility testing There is a factor of at least 10 margin between applied test levels and measured noise coupling.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
		3.1.3.6 Radiator/Air Conditioning Fans	No significant source/victim transient vulnerabilities were observed. Spike from radiator fan to O2 and brake input. The onboard coupling to throttle control signals from these sources is much less than the levels imposed during conducted susceptibility testing There is a factor of at least 10 margin between applied test levels and measured noise coupling.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
		3.1.3.7 ABS Brakes Solenoids / Motors	No significant source/victim transient vulnerabilities were observed. The onboard coupling to throttle control signals from these sources is much less than the levels imposed during conducted susceptibility testing There is a factor of at least 10 margin between applied test levels and measured noise coupling.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
		3.1.3.8 Power Mirrors / Sun Roof	No significant source/victim transient vulnerabilities were observed. The onboard coupling to throttle control signals from these sources is much less than the levels imposed during conducted susceptibility testing. There is a factor of at least 10 margins between applied test levels and measured noise coupling.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
3.2 Single Events Effects (SEE)			Faults typically induced by a Single Event Effect are covered in all the other areas. In general the throttle control electronics is protected from single event effects by the use of ASICs based on Silicon on Insulator technology and protective logic. In the event that throttle control electronics does fail, the layered defenses such as low level DTCs, hardware level over current and over temperature protection, limp home modes, and fuel cut strategies guard the vehicle against UAs. Processor and memory protection against single event effects includes EDAC on memory, data mirroring for critical variables, watch dog timer, and heartbeat functions between the two processors that check each other.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
3.3 Electro Static Discharge (ESD)			Faults typically induced by Electro Static Discharge are covered in all the other areas.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal

Environmental			Disposition	System Level Mitigations
3.4 Mechanical Vibration			No vibration testing was performed but faults typically induced by vibration are covered in all the other areas.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal
3.5 Thermal			No thermal testing was performed but faults typically induced by thermal effects are covered in all the other areas.	Disable Throttle #3 Slightly above Idle Mode Power off Throttle motor, Valve returns to spring detent 6.5° off closed. Engine Power Management through Fuel Cut based on Accelerator Pedal

B-9. Mechanical Effects

Mechanical Effects were included for completeness, but were not part of this study. Table B9-1 lists the dispositions for each element in the.

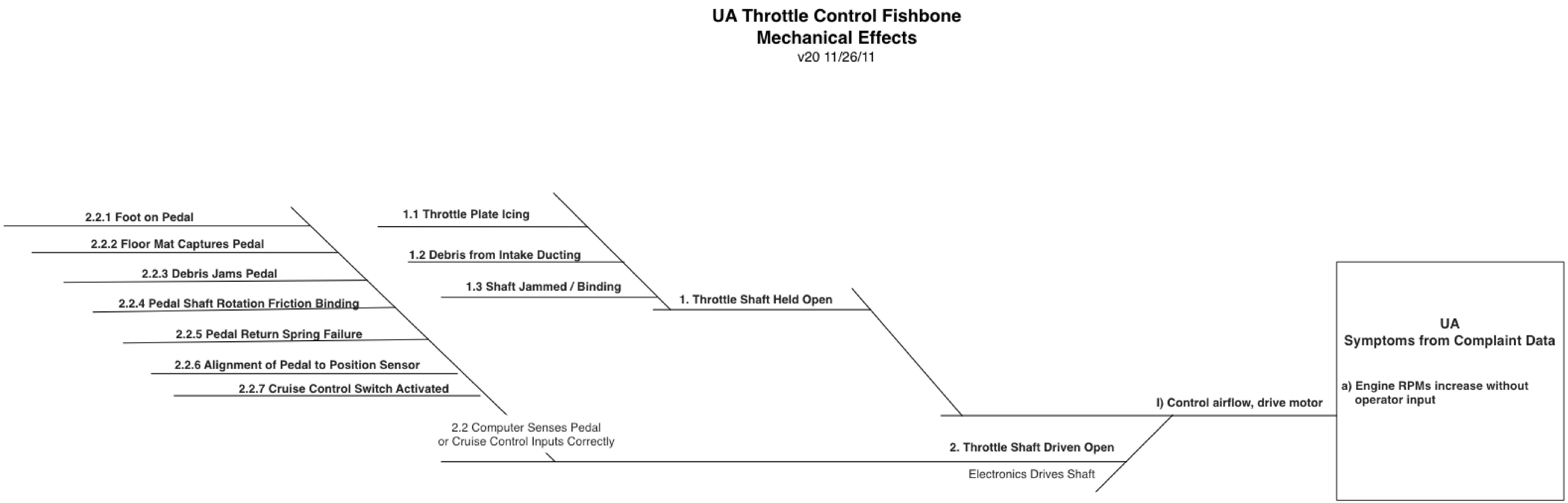

Figure B9-1. Mechanical Effects Fishbone Diagram

Table B9-1. Mechanical Effects Fishbone Summary of Design Sensitivities with Postulated Faults

Mechanical Effects		Disposition	Detection & System Level Mitigations
1. Throttle Shaft Held Open	1.1 Throttle Plate Icing	Included for completeness, not analyzed in detail	Engine Turned Off #6
	1.2 Debris from Intake Ducting	Included for completeness, not analyzed in detail	Engine Turned Off #6
	1.3 Shaft Jammed / Binding	Included for completeness, not analyzed in detail	Engine Turned Off #6
2.2 Computer Senses Pedal or Cruise Control Inputs Correctly	2.2.1 Foot on Pedal	Normal operation	
	2.2.2 Floor Mat Captures Pedal	Included for completeness, not analyzed in detail	
	2.2.3 Debris Jams Pedal	Included for completeness, not analyzed in detail	
	2.2.4 Pedal Shaft Rotation Friction Binding	Included for completeness, not analyzed in detail	
	2.2.5 Pedal Return Spring Failure	Included for completeness, not analyzed in detail	
	2.2.6 Alignment of Pedal to Position Sensor	Included for completeness, not analyzed in detail	
	2.2.7 Cruise Control Switch Activated	Normal operation	