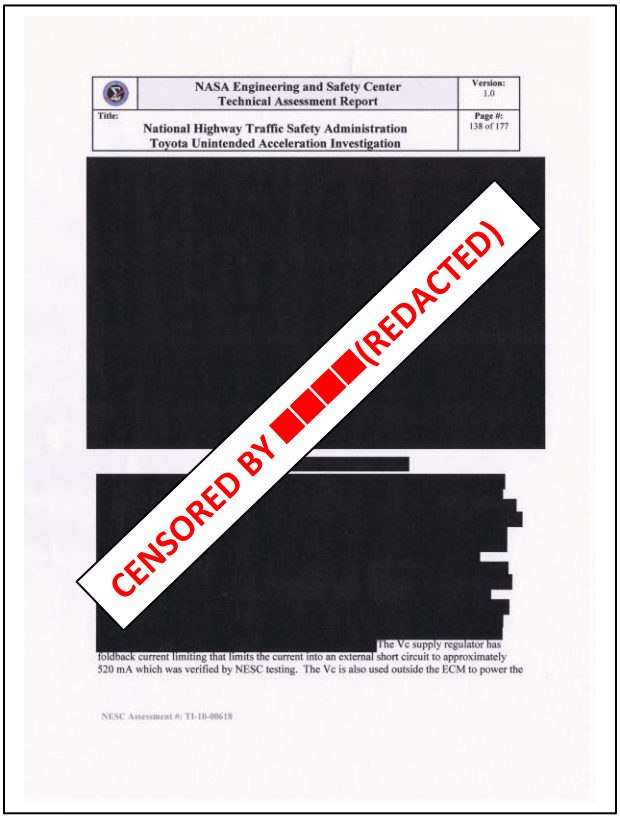


Redaction in the 2011 NASA Report

'NHTSA Toyota Unintended Acceleration Investigation'

Prepared by Dr A F Anderson CEng FIEE

antony.anderson@onyxnet.co.uk

www.antony-anderson.com

TEL +44 191 2854577

February 10th 2011

1 Background

On January 18th 2011 THE NASA Engineering and Safety Center delivered their long-awaited technical assessment report entitled 'Toyota unintended acceleration Investigation' to the National Highway Traffic Safety Administration (NHTSA).

Section 1 of the Report ' Notification and Authorisation' reads:

> Mr Daniel Smith, Department of Transportation (DOT), Senior Associate Administrator for Vehicle Safety, requested an independent assessment to determine if there are design and implementation vulnerabilities on the Toyota Motor Corporation (TMC) Electronic Throttle Control System-Intelligent (ETCS-1) that could cause unintended acceleration (UA). For the purposes of this assessment, Mr Smith is considered the primary stakeholder. Analyses and tests characterizing all identified areas of concern were performed and the NASA Engineering and Safety Center (NESC) team documented their findings, observations, and NESC recommendations in this report. The results of this study were transmitted to Mr Smith and the National Highway Traffic Safety Administration (NHTSA).
>
> This NES activity was approved by the NESC Director on March 4th 2010. The Assessment Plan was approved by the NESC Review Board (NRB) on May 20,2010. The Authority and Parties for this activity are documented in a Fully Reimbursable Space Act Agreement between the NHTSA and NASA IA1-1045 approved April 12, 2010, and in a subsequent Partially Reimbursable Space Act Agreement, IA1-1081 approved August 13, 2010.

2 Censorship in the Report

On Tuesday, February 18, 2011 the results of the NASA report were made public by NHTSA and the Report itself was published as the "Complete Report" on the internet at:

http://www.nhtsa.gov/UA

In the version of the NASA report published by NHTSA there are numerous places where the censor's black pen has redacted a number , the details of a component, obscured a key part of an explanatory diagram, blocked out sentences or paragraphs, in one case blocked out a technical reference and, in another case, an entire page. There are four appendices and in three out of the four - Software; Fishbone Diagrams; Hardware – there has been very extensive redaction.

I have gone through the report itself and in Table 1 have listed the page numbers on which these redactions occur.

Following Table I, I show a few examples, with comments underneath.

3 Discussion

In my career as an electrical industrial research and development engineer and electrical consultant I have read many technical and scientific reports and I have been the author of more than a few electrical failure investigation reports. I have never seen such a blatant case of hiding key information as this report. The net effect of the evident censorship by NHTSA is to cast a long shadow of doubt on the report itself. Whose interests does such secrecy serve? Certainly not the general motoring public who through their taxes paid to get the work done.

How can anyone properly appraise a technical report when it has been censored and emasculated in this way?

Why would anyone want to censor a report, unless it contained information that might lead to conclusions other than those that the censor might wish to be drawn?

4 Conclusions

The areas of the report which are most heavily censored are clearly those areas where problems of some kind related to sudden acceleration are most likely to be found. Those areas that I have identified so far are:

- The electronic throttle motor controller (H Bridge), perhaps associated with lock up;
- Power errors, especially those related to feeding of sensors. (Transient disturbances may affect several sensors at the same time);
- Power errors to the CAN bus;
- The cruise control –failure to disengage cruise control for example;
- Pedal command learning errors (disobedient accelerator pedal syndrome?)

There will be other areas identifiable from the Software, Fishbone and Hardware Appendices.

Regarding the censored report as it currently stands, some intensive reading between the lines is called for and will probably prove rewarding. In my opinion NHTSA may have fallen victim to the law of unintended consequences by censoring what Toyota does not want to be known.

This is a technical report of the highest importance for the future safety of millions of motorists worldwide**.** Censorship undermines the work carried out by NASA**.** Only with free and open discussion of the full contents of the report will the state of the art regarding the causes of sudden acceleration be advanced**.**

In my opinion it is of prime importance that the whole of the report and its appendices be placed in the public domain.

Antony Anderson February 10th 2011

Table 1 – List of Redactions in NASA Report ' NHTSA Toyota Unintended Acceleration Investigation'

Page	Ref	Detail	Comments
07	INDEX	Figure 6. 6.7-1 Power Supply ■■■■■.....p 138	See p 138
54	6.4.1.2	(a) The ASIC contains ■■■■ to detect high motor current and…	AFA Presumably high motor current will be either in the event of an armature flashover or stall at WOT. Why the need for secrecy about XXXX
54		(b) Two sentences blacked out	Why blackout about analog signals used by the main CPU and about the non-volatile ROM for software code and volatile static RAM (SRAM)?
56	6.4.1.2	(c) Sub-CPU ASIC 5 black outs	Why the need to black out numbers?
57	6.4.1.2	(C) Sub-CPU ASIC 3 black outs	Some differences in the MY 2005 Camry that someone seems to want to keep quiet about?
57	6.4.1.2	Sub-CPU ASIC (d) Power Control and Monitor 1 ½ lines plus one blackout	Why the secrecy about multiple regulated power supplies. Could it be that some are shared which should not be? Some interesting possibilities here that someone does not want to get into the public domain
61	6.4.3	Table 6.4.3-1 Hardware configuration evolution. Camry's Electronics Throttle Control (ETC) Evolution Summary: relating to the motor Drive Circuit.	Evidently a change of some kind in mid 2003 model year. Why the need to hide anything to do with hardware configuration evolution?
62		6) Main ASICS 2 blackouts	Differences between 2005 and 2007 Model years. What are the differences and what could be the significance?
70	Fig 6.5.1-1	System Redundancy Diagram: 4 blackouts including Power Control and Monitor	Surely there should be no need to hide anything about redundancy. Unless there are some shortcomings that you want to hide. If your reserve parachute is in good order, you don't want to censor the fact!
75	Fig 6.5.2.2-2	System Level Functional Fault tree: Lower levels blacked out	Why hide the lower levels of a fault tree unless this might give the game away and show that Toyota and consequently NASA know more than they say.
76		Reference to Table 6.5.2.2-1: number of degrees blocked out	Why is it so important that the number of degrees is not made known?
77	Table 6.5.2.2-1	Summary ETCS-I Failure Modes Evidence and Responses: Column 6 bottom number blacked out	Why hide part of a failure modes analysis?
84	Fig 6.6.1	Ishikawa or Fishbone Diagram of Postulated UA causes: 12 contributory factors partially or completely blacked out.	Makes the diagram meaningless. Note that it is the part to do with loss of power.
87	6.6.1.1	Throttle Position Control Functional Area 6.6.1.1 Detailed Implementation: Fig 6.6.1.1-1 Throttle Valve Control Block Diagram one area blacked out. 4 blackouts in description below diagram	Why, considering that it is the electronic throttle that this whole investigation is about, black out part of the functional diagram? Is there some kind of functional deficiency that someone does not wish to draw attention to
88	6.6.1.1	Throttle Position Control Functional Area 6.6.1.1 Detailed Implementation : 6 blackouts in text	
90		5 blackouts (one of these is a paragraph)	
91		4 blackouts	
92	6.6.1.2.2	Postulated throttle Position Sensors Return (E2) Increased resistance with learning: 2 blackouts (degrees)	The whole subject of "increased resistance with learning" could be rather interesting and might possibly bear on the quality of the design – so why is it left out?
97		Postulated throttle Position Sensors Return (E2) Increased resistance with learning: Blacked out range for VPA2	
100	6.6.2.2.1	Postulated Pedal Position Sensors Supply (Vc) Increased Resistance with Learning: 7 blackouts	
102	6.6.2.2.2	Postulated Faults placing VPA1 and VPA2 in the operational lane:	

		2 blackouts	
133	Fig 6.6.4-1	Cruise Control Block Diagram: 1 blackout. Text below one blackout	Why should part of the block diagram be blacked out? What is there to know here that somebody does not wish to be known
135	Table 6.6.4-3	Cruise Control Diagnostic Codes :Blackouts re P0500, P0503,P0607 especially the 0607 : Cruise cancellation Circuit Abnormal	Why black out information regarding black out codes unless this is a matter of some importance that you do not wish to be known. If the cruise cancellation circuit is abnormal, it could mean that the cruise control will fail to disengage under some conditions which is tantamount to a very dangerous situation
137	6.6.6	VSC Functional Area: 1 blackout	
138	6.6.7.1	ECM Power System : 6.6.7.1 Detailed implementation Description Almost the entire page blacked out -presumably a diagram "Fig 6.6.7-1" and text	SEE INDEX P7 WHICH REFERS TO Fig 6.6.7-1 What was in the diagram that required that it be covered up and hidden from view? Presumably Toyota did not want anyone outside NASA to see the diagram.
139	6.6.7.1	Approx. 6 lines blacked out	
139	6.6.7.2	Power system sensitivities and postulated faults: 5 ½ lines of text blacked out	Again black out on power system – why?
141	6.7.1.1.1	Pedal Command: from "to learn a lower value…" 13 lines blacked out	Isn't failure to learn something
143	6.7.1.1.6	Control Throttle Motor learnt value adjustment : blacked out. Bottom paragraph blacked out	
144	6.7.1.3	ECM software Implementation: 1 blackout and Table 6.7.4-1 blocked out	
144	6.7.1.3	ECM software Implementation: Reference 23 blacked out.	
145	6.7.1.3	ECM software Implementation : 4 short blackouts and one of 14 lines	
146	6.7.2.5	Watch Dog Timer: 3 lines blacked out	
146	6.7.3.5	Data Transfer: refreshment rate in ms blacked out	
147	6.7.3	Software study and results: msec value blacked out	

Figures 1-9

Examples of Redaction

Pages 61 – 141

With Comments

Table 6.4.3-1. Hardware Configuration Evolution

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

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

Fig 1 - Page 61 Table 6.4.3-1 Hardware Configuration Summary

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

Comment

Clearly there have been changes in the H Bridge for the Throttle Motor Drive Circuit in the middle of the 2003 model year on the V6 engine version. Why should it be that all the configuration information for the H Bridge has been blacked out on the diagram. Note the paragraph below. Why was it necessary to black out the information? Somebody seems to think that this hardware configuration information should be kept under wraps. Why?

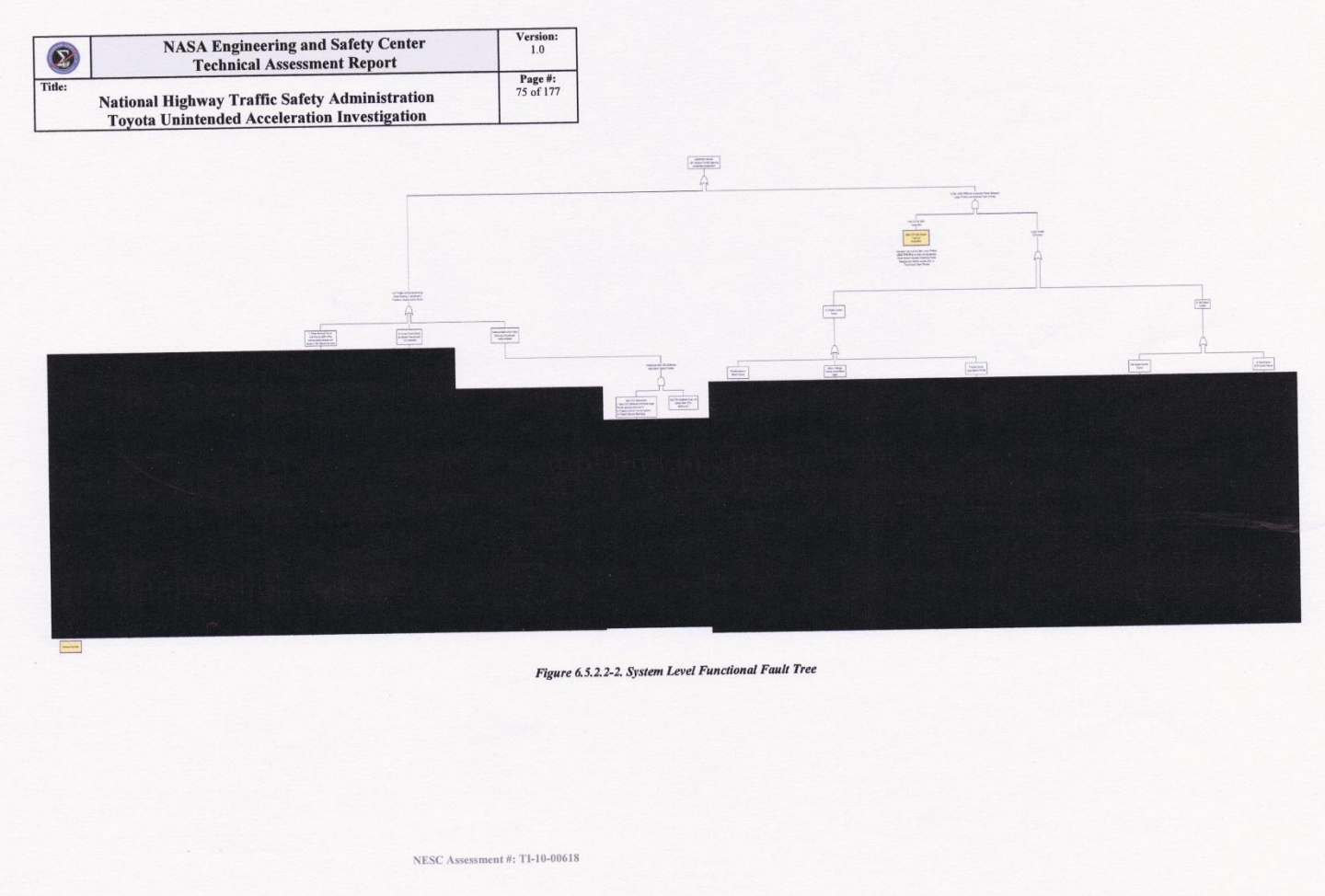
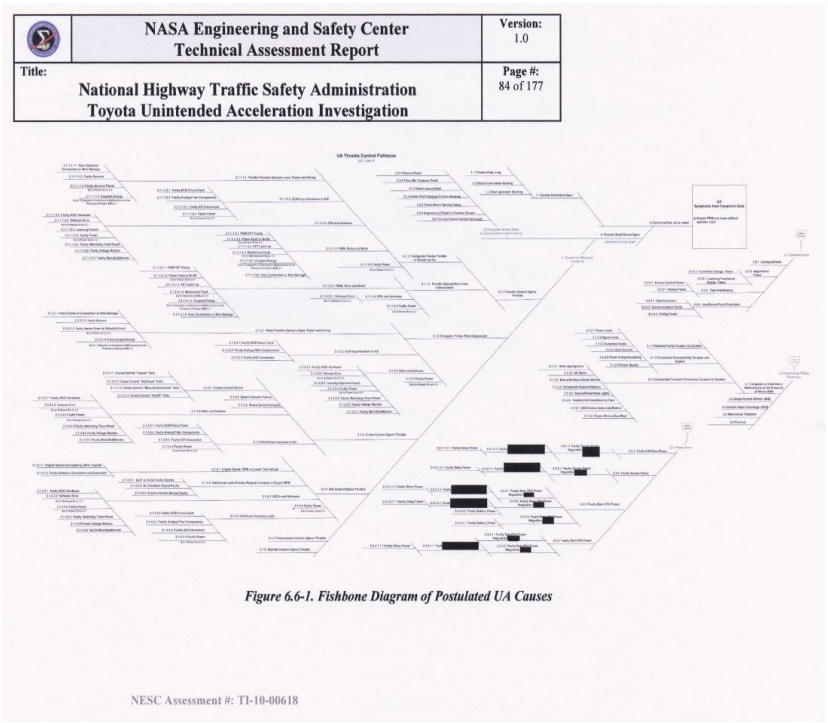


Fig 2 Page 75 – Fig 6.5.2.2-2 System Level Functional Fault Tree

What use is a fault tree like this?



NASA Engineering and Safety Center Technical Assessment Report | Version: 1.0

Title: National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation | Page #: 84 of 177

Figure 6.6-1. Fishbone Diagram of Postulated UA Causes

NESC Assessment #: TI-10-00618

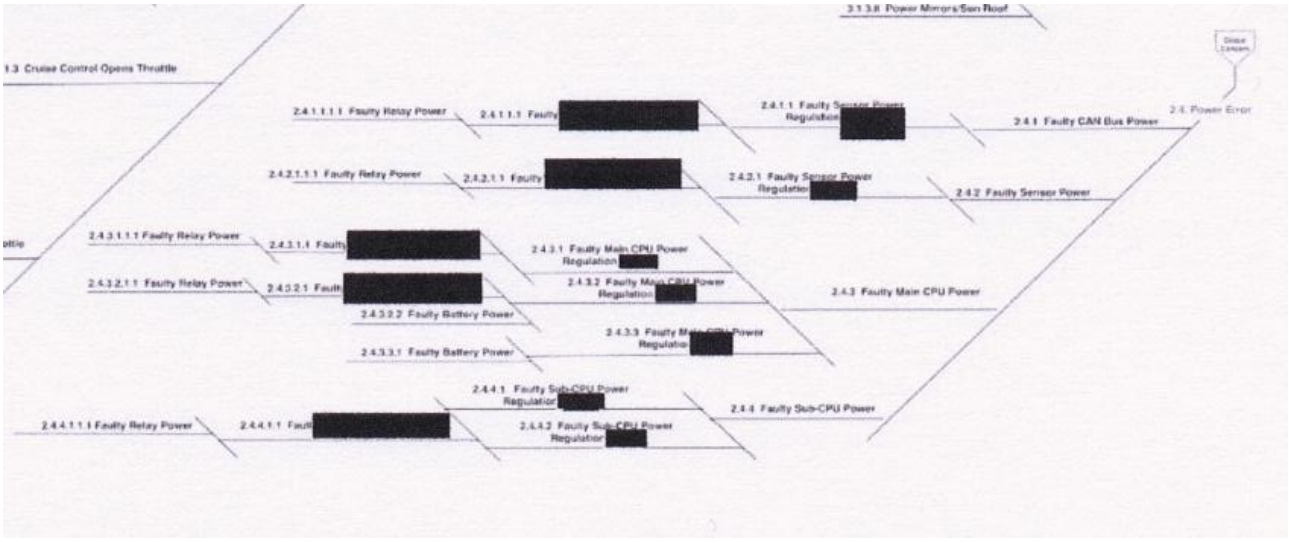


Fig 3 Page 84 Part of Figure 6.6.1 – Section 2.4 Power Error portion of Ishikawa or fishbone Diagram for Postulated causes of Uncommanded Acceleration

Comment:

Why should anyone want to hide the power error portion of a diagram that relates cause and effect? Surely, was not the object of the whole investigation to identify possible causes of sudden acceleration and prove or disprove them? Here some of the possible causes of sudden acceleration and their interactions are being **hidden** from public view. This looks like a case of trying to put the cat back into the bag.

"sub cut" and "main cut" in the block diagram). [redacted] The other [redacted] FETs are a part of an H-Bridge that switches either side of the motor winding to ground in response to PWM signals [redacted] from the Main CPU at approximately 500 Hz. The other two H-Bridge FETs PWM switch the +12V power and these are located inside the IC. [redacted]

The IC also has a signal from the Sub-CPU and a different signal from the Main CPU that can inhibit PWM drive signals to the H-Bridge, as shown as inputs to the Motor Drive I.C. in Figure 6.6.1.1-1. Also, certain sensed voltage conditions can trigger an IC reset with PWM drive signal inhibit. [redacted]

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

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

Fig 4 Page 88

Comment

Why is so much effort being put into blacking out information about the operation of the H Bridge? An H Bridge drive is entirely standard technology and has been for years for reversing DC motor drives. There is no proprietary information here. Could it be that there is a latch up problem with the H Bridge that NASA have uncovered with the help of Mr Ron Belt that NHTSA are now trying to hide?

6.6.1 Throttle Position Control Functional Area

6.6.1.1 Detailed Implementation Description

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

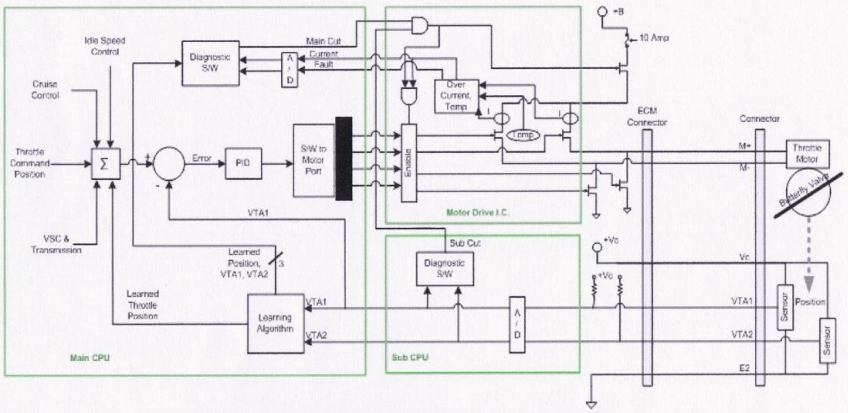


Figure 6.6.1.1-1. Throttle Valve Control Block Diagram

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

Power to the throttle motor is controlled by the Main CPU via the Motor Drive IC and [redacted] FET switches. One [redacted] FET switch is in series with fused +12V drive power to the IC and can be switched on or off by either the Main or Sub-CPU (as notionally represented as

Fig 5 Page 87

Comment

NASA presumably wanted to explain how the electronic throttle system worked, but NHTSA seems to have decided, for reasons best known to itself, to hide that information. Why is it necessary to hide the way the throttle system works?

Table 6.6.4-3. Cruise Control Diagnostic Codes

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

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

Table 6.6.4-4. Cruise Control Auto Cancel

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

6.6.4.2 Cruise Control System Sensitivities and Postulated Faults

The software study focused on the following:

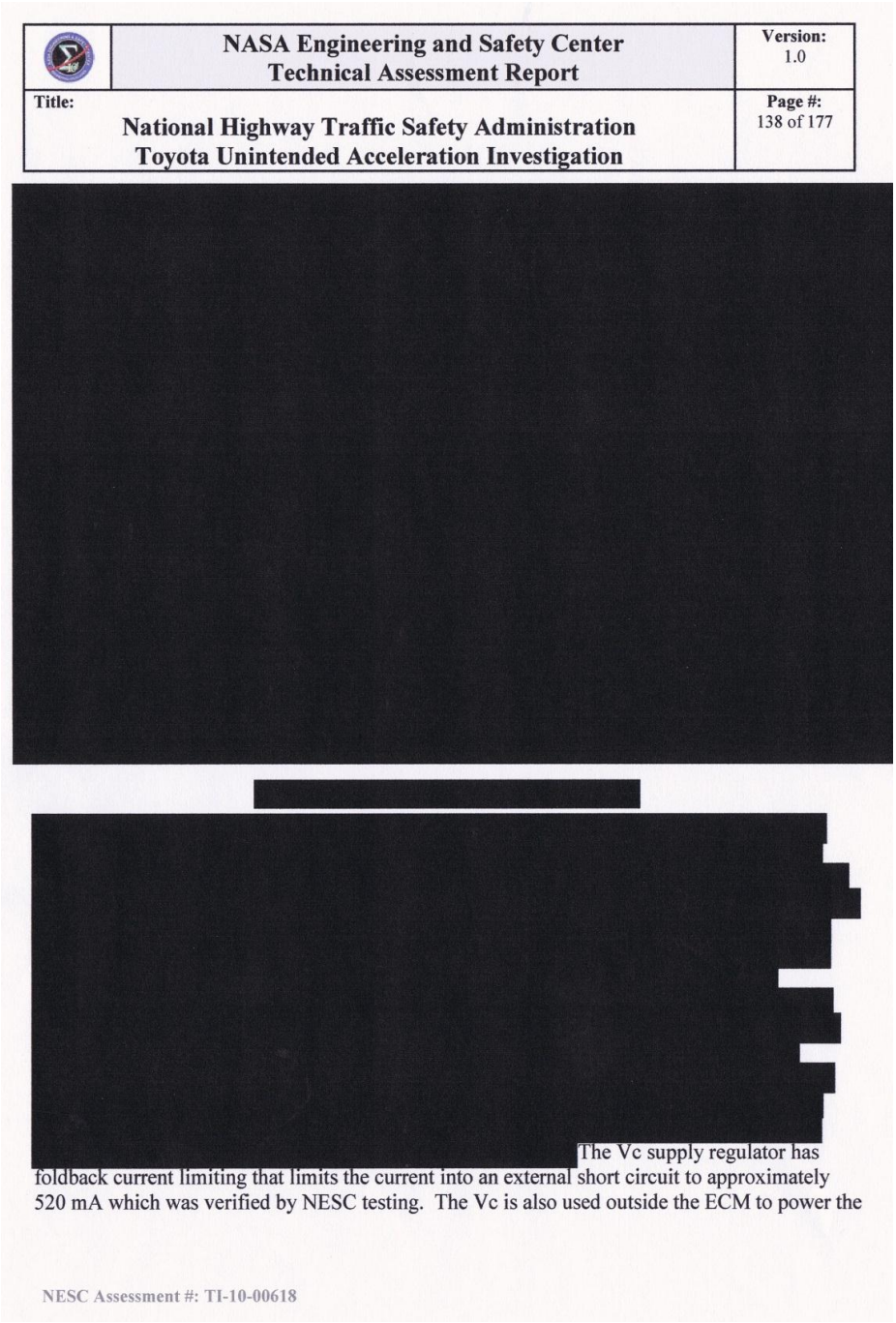
1. Failure modes of the cruise control switch that causes an acceleration behavior and no DTC or indication.
2. Failure modes that prevent the cruise control from being reset or cancelled.
3. Failure of the speed sensors.

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

Fig 6 Page 135 Diagnostic Codes.

Comment

Why is it necessary to hide information relating to the diagnostic codes? What is it about P0697 that is of such significance that it has to be hidden?



NASA Engineering and Safety Center
Technical Assessment Report

Version: 1.0

Title:
National Highway Traffic Safety Administration
Toyota Unintended Acceleration Investigation

Page #: 138 of 177

[redacted]

[redacted]

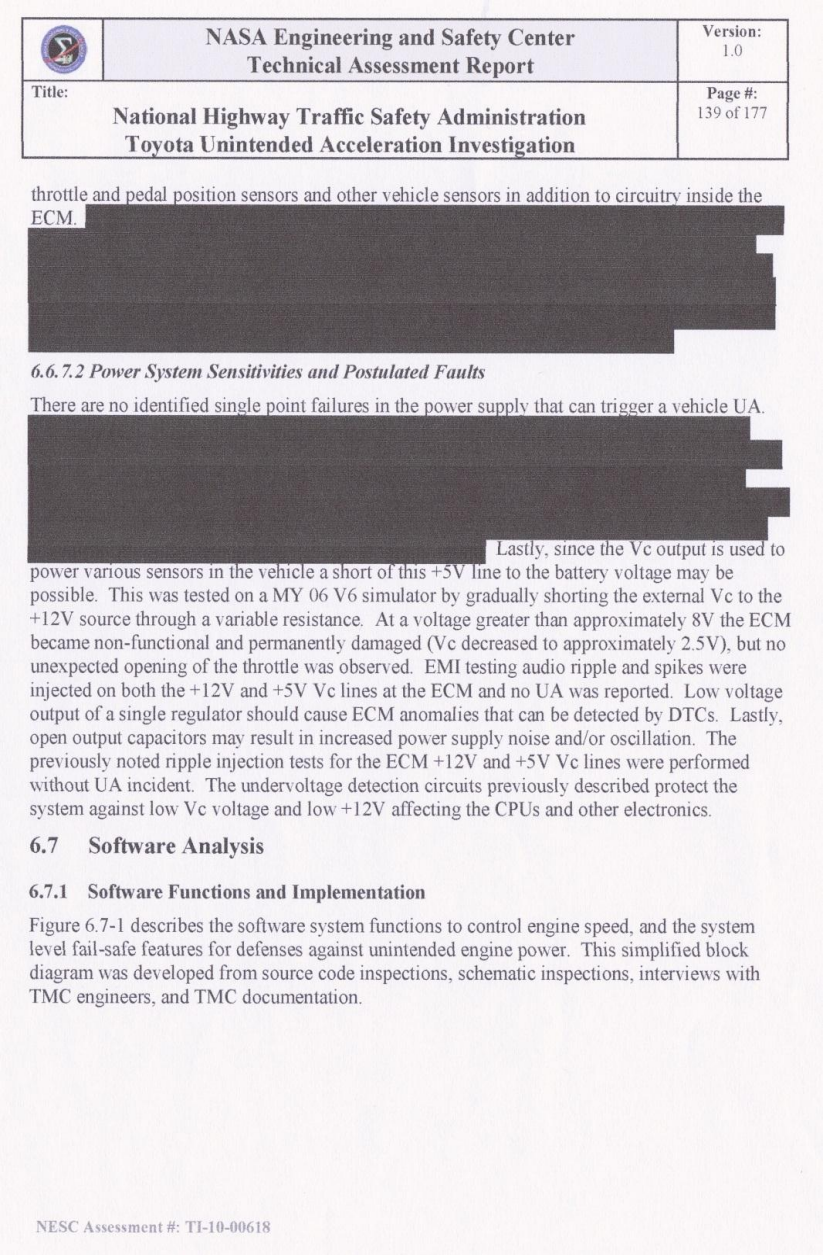
The Vc supply regulator has foldback current limiting that limits the current into an external short circuit to approximately 520 mA which was verified by NESC testing. The Vc is also used outside the ECM to power the

NESC Assessment #: TI-10-00618

Fig 7 Page 138 Relates to ECM Power System

Comment

Why is it necessary to hide almost all the information about the ECM Power System? Note that Vc is used to power both pedal sensors and both throttle sensors AND other vehicle sensors. As I understand it, the accelerator pedal sensors are supposed to be driven from independent supplies, likewise the throttle sensors. Here we have all four driven from the same supply.



NASA Engineering and Safety Center
Technical Assessment Report

Version: 1.0

Title:
National Highway Traffic Safety Administration
Toyota Unintended Acceleration Investigation

Page #: 139 of 177

throttle and pedal position sensors and other vehicle sensors in addition to circuitry inside the ECM. [redacted]

6.6.7.2 Power System Sensitivities and Postulated Faults

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

6.7 Software Analysis

6.7.1 Software Functions and Implementation

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

NESC Assessment #: TI-10-00618

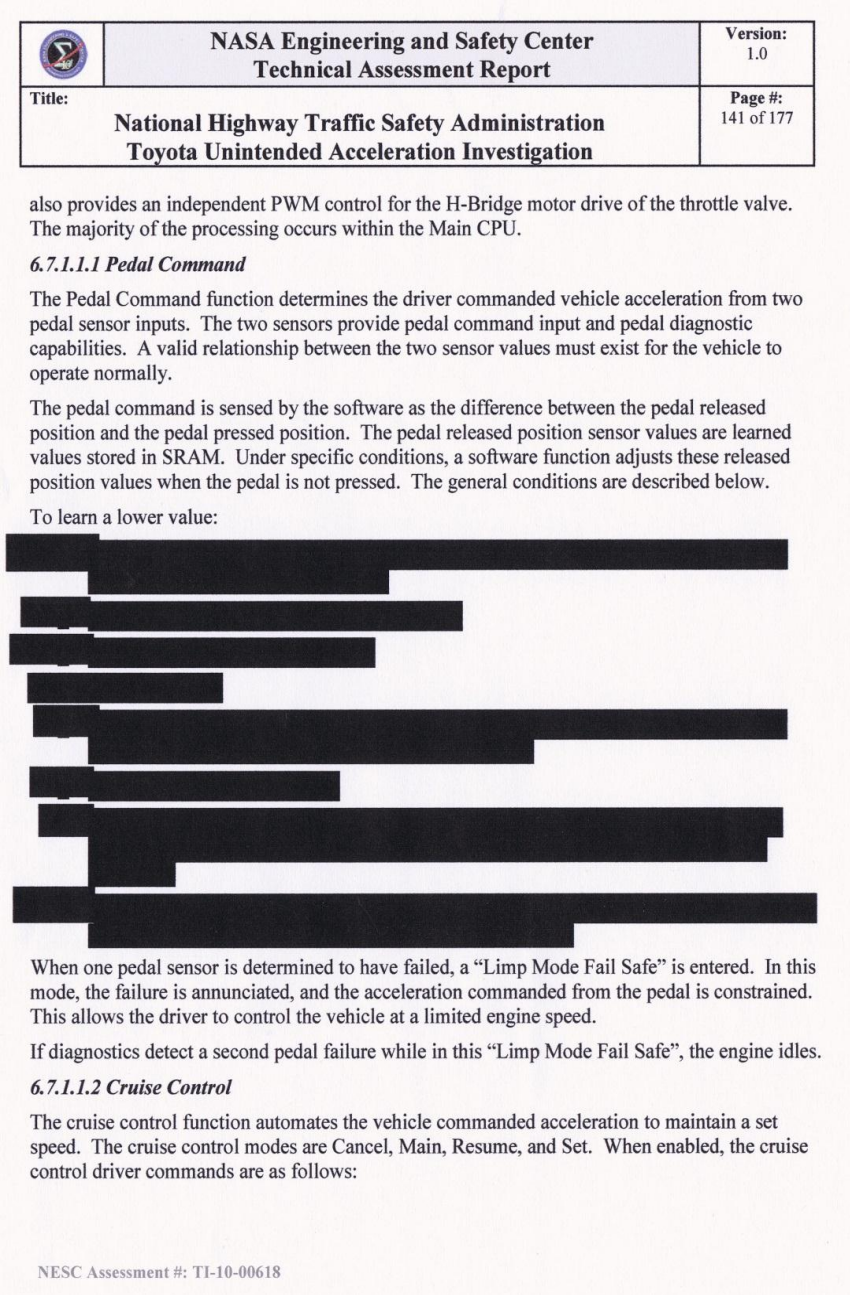
Fig 8 Page 139 Relates to ECM Power System

Comment:

Why is it necessary to blank out information relating to the power supply to the pedal position sensors and other vehicle sensors? See also fishbone diagram Fig 3.

Why is it necessary to block out information about Power System sensitivities and postulated faults?

It has come to a pretty pass when information about postulated faults is blacked out! We don't want you to know about what NASA considered might be possible faults. Surely the opposite ought to be the case, i.e. you tell everyone exactly what postulated faults you have considered!



NASA Engineering and Safety Center
Technical Assessment Report

Version: 1.0

Title:
National Highway Traffic Safety Administration
Toyota Unintended Acceleration Investigation

Page #: 141 of 177

also provides an independent PWM control for the H-Bridge motor drive of the throttle valve. The majority of the processing occurs within the Main CPU.

6.7.1.1.1 Pedal Command

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

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

To learn a lower value:

[redacted]

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

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

6.7.1.1.2 Cruise Control

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

NESC Assessment #: TI-10-00618

Fig 9 Pedal Command

Comment

Clearly there is some kind of problem with the pedal command. The pedal seemingly is supposed to "learn" to adjust to circumstances and presumably sometimes doesn't. This suggests that unlike with the conventional mechanical system the electronic linkage can change its characteristics or transfer function. If so, this blacked out section may be pregnant with hidden meaning. It is tantamount to an admission that there may be a problem with the pedal's "learning" capability. Perhaps it is dyslexic? Or has the capability of doing the opposite of what the driver's intention is? Perhaps the harder you press the pedal the more the throttle closes and the more you lift the foot the more the throttle opens. Clearly this is a possibility, albeit very unlikely!