

NHTSA 2014-0108

“REQUEST FOR COMMENT ON AUTOMOTIVE ELECTRONIC CONTROL SYSTEMS SAFETY AND SECURITY”

PERSONAL RESPONSE

BY

DR ANTONY ANDERSON CENG FIEE/FIET

INTERMITTENT ELECTRONIC/ SOFTWARE MALFUNCTIONS – LEARNING FROM FAILURES

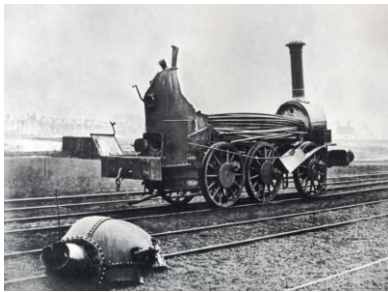


Fig 1: Examples of past engineering failures from which much has been learnt

“The obscure we see eventually. The completely obvious, it seems, takes longer.”

Edward R. Murrow (1905-1965)

“...for a successful technology, reality must take precedence over public relations, for nature cannot be fooled”.

Richard Feynman (1918-19880 on the Columbia Shuttle Disaster

“On the wreckage of thy yesterday, design thy strong structure of tomorrow.”

Ella Wheeler Wilcox (1850 –1919)

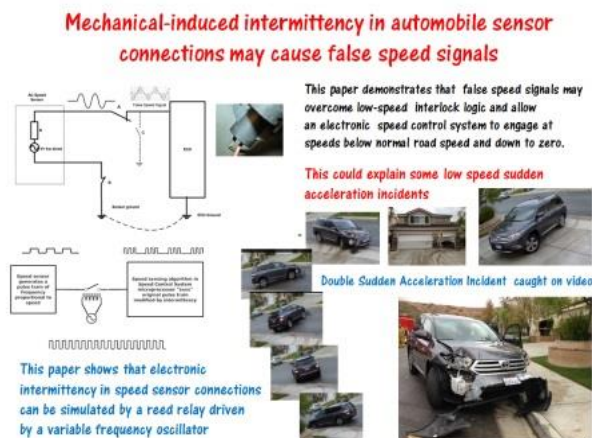
Personal introduction by [Dr Antony Anderson C.Eng FIEE/FIET MIEEE](#)



I am a UK electrical engineering consultant with an academic and industrial R & D background in electrical machines and control systems¹. I am not an automobile engineer. I offer my comments on **NHTSA 2014-0108** because I believe that the industry has a great deal to learn from other industries, such the railway industry, the metal rolling industry, the aircraft industry, to name a few, which have a far longer experience of applying functional safety standards to computer control of safety critical electronic control systems than does the automobile industry.

Over the years I have organized a number of large-scale multi-disciplinary failure investigations relating to electrical machines and their control systems, so I am aware of the need to methodically identify the root causes of failure and learn from them and of the inherent difficulties in identifying intermittent electronic/software malfunctions in control systems.

During the past 13 years, while working as an independent electrical consultant, I have investigated a number of failures in safety-critical control systems in vehicles in the UK, Ireland, Continental Europe, New Zealand and the USA. I have paid particular attention to the subject of Unintended Sudden Acceleration. In March 2014 the Institute of Electrical and Electronic Engineers journal **IEEE ACCESS** published my peer-reviewed research article [Intermittent Electrical Contact Resistance as a Contributory Factor in the Loss of Automobile Speed Control Functional Integrity](#)



My IEEE ACCESS article deals with intermittent electronic/software malfunctions in automobiles and so clearly relates to **NHTSA 2014-0108** regarding ‘Electronic Control Systems Safety and Security’. In particular, it relates to “control systems that impact throttle, braking, steering and motive power management” and it complements my comments that follow in this present memorandum. It raises issues relating to the diagnosis of No Fault Found (NFFs) in the case of intermittent electronic malfunctions and of the shortcomings of present Motor Vehicle Data Recorders (EDRs), again issues that relate to **NHTSA 2014-0108**.

[ABSTRACT OF PAPER](#)

[Download Full Text in HTML with video](#)

¹ I also have ten 10 years practical experience in organising the improvement of commercial, engineering and manufacturing, assembly, servicing and spares systems in a large heavy electrical engineering company with a product structure based “common language” for information processing and control.

1 Functional Safety in Other Industries – a brief comparison with the auto industry

In the nuclear, aerospace and non-automotive transport industries, a disciplined approach to design of control system hardware and software has increasingly become the norm. External design reviews regarding functional safety by independent qualified bodies are generally accepted as enhancing the integrity of safety critical systems. Increasingly, attention is being paid to “near miss” incidents in service because they can give early warning of potentially hazardous situations before they occur. Until now, automotive companies have kept their electronic systems design and embedded software code “under the driver’s floormat”, so to speak. Automotive safety-critical control systems and their associated software are not at present subject to external review or audit by specialist reviewers at the design stage to ensure that best practice is being followed. Current public critiquing of automobile manufacturers is very much after-the-event and tends to focus on deficiencies in the recall process. But why do recalls arise in such numbers in the first place? What is it about the automobile design, manufacturing and assembly processes that allow foreseeable problems to be built in to vehicles in the first place that will later give rise to recalls? In my opinion, as far as electronic functional safety is concerned, the automobile industry has a lot of catching up to do, see [An Open Letter to the NAS: The Poor Quality of Functional Safety Engineering in the Automobile Industry by Anderson, Kirk and Armstrong Nov 2010](#).

2 Evidence of systemic failure in the automobile design, manufacturing and service processes

Much attention is presently being devoted to identifying flaws in the automobile recall process and trying to apportion blame for its shortcomings. Attention must however also be paid to flaws in the **diagnostic processes** that failed to discover the faults that eventually led to the belated recalls. This is a particular issue with intermittent electronic/software malfunctions that are inherently difficult to pinpoint and will not necessarily be detected by current on-board diagnostic systems. EDRs too have severe limitations when it comes to determining the causes of road accidents², yet are often treated as if they are the equivalent to aircraft black boxes, which they most certainly are not.

It is scarcely surprising, bearing in mind the difficulty in diagnosing intermittent electronic malfunctions, that automotive diagnosticians tend to scapegoat the driver. Who better to blame than the driver?

In my opinion, NHTSA needs to recognize that much automotive diagnosis relating to intermittent electronic malfunctions is currently based on the fallacy that “absence of proof is proof of absence”. This is a matter that I treat at some length in my [IEEE ACCESS article](#). The fact of not finding an intermittent electronic fault may mean that the search did not go on long enough or that the diagnostic tools used were not up to the task. It should not necessarily result in transfer of blame to some non-electronic cause.

3 Interaction between the Law, the Driver and the Vehicle and the vehicle electronics

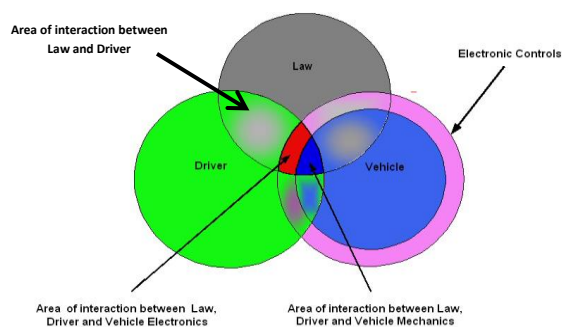


Fig 1 Interactions between Law & Regulation, Driver and Vehicle and Vehicle electronics

² See Anderson, Kirk and Armstrong “The Present Limitations of Motor Vehicle Electronic Data Recording” An open letter to the NAS Team working on the project: Electronic Vehicle Controls and Unintended Acceleration (TRB-SASP-10-03) submitted as an attachment to this comment to NHTSA 2014-0108.

Fig 1 shows a simplified representation of the interactions between the Law, the Driver, the Vehicle and the Vehicle control electronics. As the role of electronics in vehicle control systems expands, so will the red area expand. Much of this interaction will be positive: electronic speed control may enable drivers to control speed accurately and avoid speeding fines. Some interaction will be negative; a malfunctioning electronic throttle may cause an un-commanded sudden acceleration (SA) incident that results in a fatal injury. As a result the driver, not the vehicle, may well come in conflict with the law. Vehicle-to-vehicle communication may help reduce the likelihood of accidents, but it will also make it easier for malicious persons to download malware that may cause abnormal behaviour in various safety-critical control systems (throttle, steering, braking), perhaps in many vehicles, more or less at the same time. How the Law will deal with such maliciously-induced incidents, which may well appear to be caused by the driver, remains to be seen. Even as things presently stand, the law takes no account of the fact that the driver no longer controls vehicle speed by operating directly on the throttle via an accelerator pedal and a mechanical cable, but acts **indirectly** through the agency of the engine control computer that in turn controls the electronic throttle.

Consider the difference between a mechanical and an electronic throttle. Fig 3 shows a simplified comparison of a mechanical and an electronic throttle.

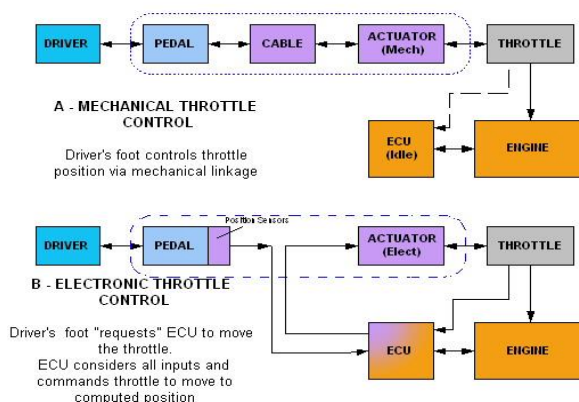


Figure 2. Comparison of (A) mechanical throttle where driver's foot controls throttle position with (B) electronic throttle where driver's foot "requests" the ECU to move the throttle.

- If the electronic throttle should cause an uncontrollable SA incident resulting in an accident, who is ultimately responsible: the driver, or the company that designed a poorly-programmed electronic throttle controller?
- Should the driver be held responsible for the consequences of a software-induced sudden acceleration, or a sudden loss of electronic steering capability?

In my opinion:

- the Law needs to adapt to take account of the fact that safety critical control systems, if they malfunction, may cause accidents for which the system designers and the automobile company that employs them should take responsibility;
- Automobile companies need to accept that their electronic control systems and embedded software have the potential to kill and that therefore they should submit their designs to third-party safety certification;
- NHTSA needs to address the misconception of automobile electronics as being "perfect, unless proved otherwise" and emphasise that automobile electronics need to be subject to third-party safety certification.

4 Bringing Order out of Disorder

In any comparatively new field, such as electronics and software, and particularly with software, innovation tends to come first, and systemization follows later. In this respect Professor Nancy Leveson's paper [High Pressure Steam Engines and Computer Software](#) provides a very useful and readable historical perspective. She writes in her introduction:

“The introduction of computers into the control of potentially dangerous devices has led to a growing awareness of the possible contribution of software to serious accidents. The number of computer-related accidents so far has been small due to the restraint that has been shown in introducing them into safety-critical control loops. However, as the economic and technological benefits of using computers become more widely accepted, their use is increasing dramatically. We need to ensure that computers are introduced into safety-critical systems in the most responsible way possible and at a speed that does not expose people to undue risk.

Risk induced by technological innovation existed long before computers; this is not the first time that humans have come up with an extremely useful technology that is potentially dangerous. We can learn from the past before we repeat the same mistakes. In particular, parallels exist between the early development of high-pressure steam engines and software engineering that we can apply to the use of computers in complex systems.”

Automobile software architecture and coding practice *ought* to follow best industrial practice, but this is not necessarily the case. Getting the design right in the first place is essential for software and can only be done if design is approached in a systematic rather than an ad-hoc manner. **Hence the need in the automotive context for the application of the principles of ISO 26262. In my opinion, this is a matter to which NHTSA could and should usefully direct the attention of the automobile companies in a forceful manner.**

5 The matter of trust regarding the automobile – then and now

Vehicles sold today are unquestionably much more reliable than in days gone by. The manufacturers will say: “Trust us! We’ve tested our vehicle electronics and software to exhaustion... if by any chance you have any problems, we will sort them out.” Customers buy on such promises. All goes well for a while and, for most drivers, all of the time. Then comes the day when one driver, reports some unpredictable, anomalous vehicle behaviour. It might be an unexpected engine surge or a full-blown sudden acceleration or an un-commanded engine switch off. The mechanic takes the vehicle into the workshop. He gives it a visual check-over. He wiggles the wiring harness. He tests the brakes and steering and he looks for any fault codes on the diagnostic system. He takes the vehicle for a ten minute test drive. He finds nothing.

The dealer then says to the customer: “Very sorry! The mechanic can’t find anything wrong with the vehicle. No fault codes show up. We haven’t had any complaints exactly like yours. (Note the little qualifier *exactly*. No two circumstances are ever *exactly* alike, are they?) He may say “If it happens again bring it in and we will have another look at it”. Or else he may say: “we can’t do anything unless the fault can be reproduced”³. The dealer suggests to the driver, albeit indirectly and in the politest words, that he is either imagining things or telling a pack of lies. In effect he says; “Prove, or reproduce, the alleged intermittent malfunction, or else accept that you imagined the incident or that it was the result of your own driving error.”

Because the dealer has found nothing, there is no cause to contact the manufacturer, unless there is built into the Dealer Fault Reporting System a means of recording and reporting No Fault Found (NFF) diagnoses. As

³ For example in one complaint in the NHTSA complaints database [ODI 10201655], the driver recorded five alleged SA incidents in a few months. After the second incident, the dealer reported ‘no fault found’(NFF) and after the third said ‘We can’t fix the problem until we can duplicate it’. The fifth SA incident resulted in a rollover and smash-up from which the driver was lucky to come out alive. It occurred on the journey to the garage for a diagnostic check-up following the fourth incident. Neither NHTSA nor the manufacturer followed up on these incidents.

a result, the feedback loop to the manufacturer from the field may fail and, as a consequence, the manufacturer will not necessarily get early warning of safety critical problems. The NHTSA ODI complaints database is full of complaints of failure to diagnose the cause of the complaint. There is clearly a need for more effective diagnosis regarding NFFs which are inadequately handled by existing on-board diagnostic systems and workshop diagnosis. There is also a need to report NFFs as “known unknowns” both to manufacturers and to NHTSA.

The reporting of NFFs, which surely is also connected with better early warning systems, could probably be improved by better diagnostic training within the automobile industry. But that will only come about when the fallacious “Absence of proof is proof of absence” diagnostic argument, already mentioned, is exposed and is replaced by “Absence of proof is not proof of absence”. Regarding NFFs, the automobile diagnostician in such instances should be encouraged to keep an open mind and not to reach any premature conclusions, pending further evidence.

In my opinion there is a need for:

- **better methods of determining when an electronic intermittency has occurred;**
- **Ways of describing and recording NFFs, “known unknowns”, so that they do not get lost or become wrongly attributed;**
- **better methods of recording alleged intermittent malfunctions in both the NHTSA ODI database and Manufacturer’s service databases.**

6 The automobile industry is accountable only to itself regarding electronic functional safety

The automobile industry, unlike other safety critical industries, is given an enormous amount of freedom to be **accountable only to itself**. Theoretically customers have the collective power to call auto manufacturers to account. But, in practice, the automobile industry isolates each customer complainant and makes them feel as if they are completely on their own. In effect, the supplier-customer relationship is out of balance, with the supplier holding most of the cards in his hands. In the case of the automobile, the owner has very little information about the product available to him. The owner’s manual, workshop manual and a wiring manual tell the reader nothing of importance about the various electronic systems and how they interact. Therefore the owner is at a tremendous disadvantage vis-à-vis the dealer and the manufacturer. Where the evidence in litigation points strongly to an electronic malfunction, it is likely that the manufacturer will settle before trial and will therefore be able to keep any discovered evidence under wraps.

In other industries the customer has far more clout. When there is a failure it is usually in everyone’s interest to get to the bottom of the problem quickly and no mileage in hiding possible causes: nobody wants a repeat occurrence because the lost revenue to the customer and risk of loss or reputation to the supplier are far too great **not** to investigate. Where there is a failure there will usually be a proper forensic investigation to establish, where possible, the likely cause and make recommendations as to what remedial/preventive action needs to be taken.

This issue of accountability in matters of functional safety is one that properly should concern NHTSA.

7 Electronic functional safety has to be built in from the outset, not added on later

In other industries it is assumed that Murphy’s Law is applicable (whatever can go wrong will). There is therefore a duty of care incumbent upon the manufacturer to anticipate the operation Murphy’s Law and take preventive measures against its operation. It seems to me that the auto industry, does not yet really recognize the universality of Murphy’s law and that functional safety, especially for safety critical automotive electronic and electrical systems, has to be built into designs **from the outset** and must form an integral part of each automotive product development phase, ranging from the specification, through design, implementation, integration, verification, validation, and production release. There are many examples where, with the benefit of hindsight, if simple practical preventive measures had been adopted at the design stage a problem would never have arisen in the first place. For example:

- the under hood fire problem that afflicted some Ford vehicles fitted with next-generation cruise control systems.⁴
- The electronic throttle problem. If an independent functional safety review had been carried out **before** the first electronic throttle was introduced, it would have determined that an independent kill switch, or equivalent, was an absolute necessity. As a result, the number of sudden acceleration incidents resulting in death or injury would have been minimal.

One of the purposes of ISO 26262 is to put in place design review procedures to identify such problems in a systematic way and so put in place preventive measures. To do this requires an open admission of past failures so that lessons can be learnt from them. However for the automobile industry to change to a culture where failures are hidden to one where they are acknowledged and learnt from will require major changes. In my opinion, the question for NHTSA is how best to assist in bringing about this very necessary culture change.

I think that NHTSA could quite properly address the following questions:

- **how is a cultural change to be engineered in the automotive culture in which electronic functional safety is given its proper weight?**
- **How are staff both in NHTSA and in the automobile industry to be persuaded to accept that Murphy's law (whatever can go wrong will) applies to the functional safety aspects of automobile electronics and software and that it is their responsibility to ensure that all reasonable efforts to mitigate the potential consequences of its operation?**

8 Feedback of complaints – the imperfect nature of present processes

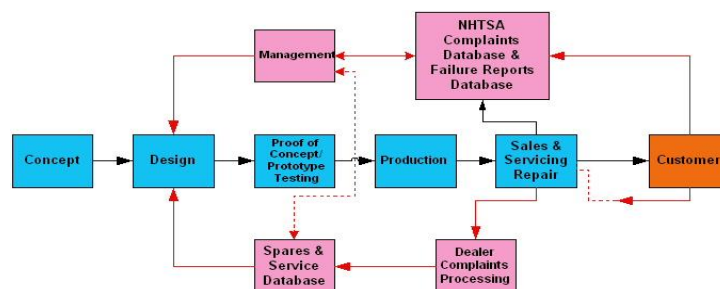


Figure 3. Idealized feedback of complaints data to Design via Dealer Network and NHTSA

The above figure shows a simplified and idealized picture of how customer complaints are fed back in several different ways into the design process.

⁴ The designers, for US built cars, had incorporated a safety feature in the form of a brake pressure switch which, when the brakes were pressed full, opened a switch to disable the cruise control. The positive side of the switch was connected to a 12V supply that was always hot. Eventually, the flexible Kapton membrane would rupture that separated the high pressure side of the switch from the low pressure switching side. Hydraulic fluid would then leak into the switching space. The positive side of the switch and the earthed casing now formed, with the hydraulic fluid, a 12V electrolytic cell. This allowed the build-up of dendrites between the positive side of the switch and ground that tended, over time, to short circuit the switch. However, vehicle engine vibration and motion broke up the dendrites and it was only when the vehicle was stationary, with the engine switched off, that the switch could go to a full short circuit. Had the fuse been properly designed, it would have fused and protected the switch, which could have been replaced at the next servicing. However, instead of a 2A fuse a 10A or even a 15 A fuse was used, for no discernible reason. When the fault occurred the current built up and caused a hotspot that ignited the hydraulic fluid in the switch, which, in turn set fire to the hydraulic reservoir on top of the master cylinder, which then ignited the magnesium alloy body of the master cylinder, causing a spectacularly violent under-hood fire. It was not until about six hundred under-hood fires had been reported that there was finally a recall. Eventually of over 6 million vehicles were recalled, or so I believe. This huge expense could have been saved by simple attention to following simple rules of protection: protect the pressure switch by a low amperage fuse and/or a current limiting resistor in the positive lead to the switch. However, the recall notice never reached Bogota Colombia, where in 2007 I disabled the deactivation switch in a Ford F150, thereby pre-empting the possibility of catastrophic fire in an electrical machine rewind shop where the vehicle was often parked, and where there was no shortage of inflammable material.

- The customer may register his complaint with the Dealer by putting his vehicle in for servicing and repair and the complaint gets processed and in due course changes gets fed back into design.
- The customer may also lodge a complaint on the NHTSA ODI Complaints Database.

Both these processes are imperfect and are very slow in their effect and need improvement. I think this could be achieved with a better computer- assisted methodology for establishing the essential attributes of particular complaints and a database structure that allows for better epidemiological studies and comparisons.

In September 2001, Toyota introduced the XV30 model Camry (Model years 2002-2006). This was the first Camry to be fitted with an electronic throttle. In my opinion, the rise in SA complaints for the Camry should have been apparent both to Toyota via feedback from its dealers and to NHTSA via its complaints database during 2002 and should have set alarm bells ringing in both camps. As can be seen from Fig. 6.2.3-1 in the 2011 NASA Sudden Acceleration Report commissioned by NHTSA, reproduced as Fig. 4 following, the introduction of the electronic throttle in the Camry and other Toyota vehicles produced a sharp rise in complaints of sudden acceleration (SA) incidents to NHTSA.

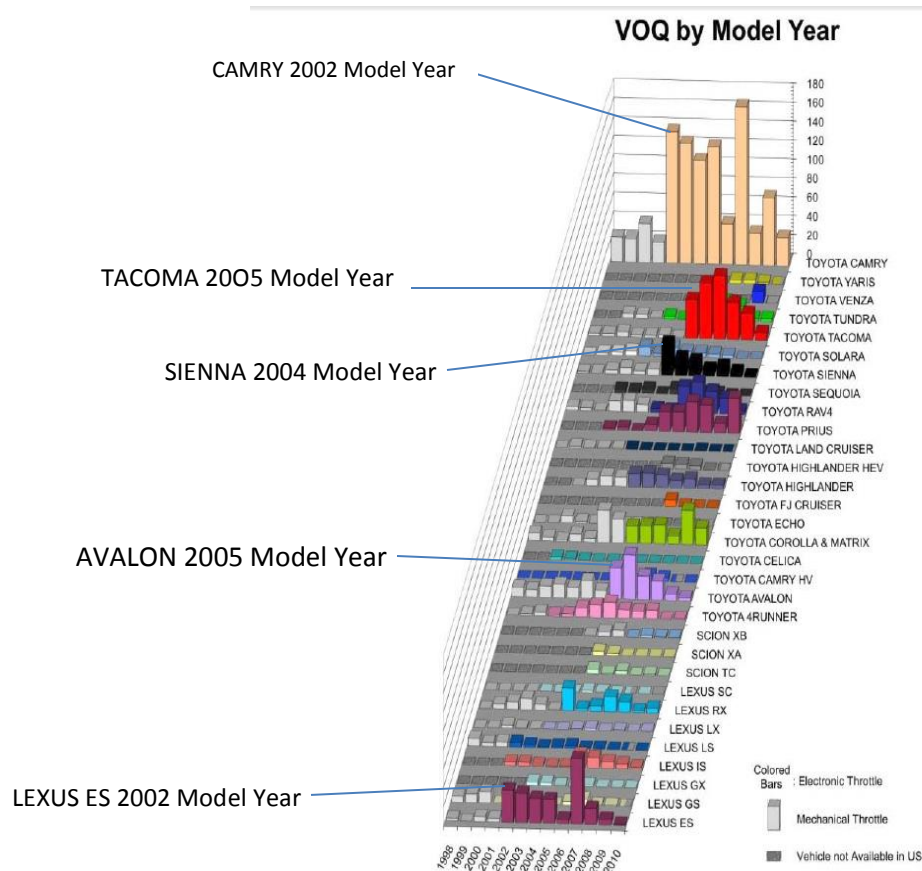


Figure 6.2.3-1. Number of VOQs by TMC Vehicle Model and MY
Grey bar indicates mechanical throttle, Colored Bar indicates ETCS-i throttle

Figure 4. Diagram that illustrates useful information regarding SA incidence in different Toyota models by model year that can be extracted from existing NHTSA VOQ Database even as it presently exists.

This diagram shows that, with difficulty, it is possible to extract significant comparative information from the NHTSA ODI Database. This analysis was carried out in 2010 it would still have shown significant trends if carried out four years earlier. However if it had been possible to gather information in a structured manner to a greater depth, this would have allowed far finer analysis to be carried out and more rapidly.

In my opinion, the NHTSA ODI complaints database does not record data to a sufficient level of detail to allow proper epidemiological studies to be carried out. For example, complaints are categorised as to what vehicle component or part they appear to relate, but those categories do not appear to correspond with the categorizations used by the motor manufacturers to break down the automobile into its component assemblies, sub-assemblies, systems and sub-systems etc. Some of the categories are catchalls: for example “UNKNOWN, OR OTHER”. The data model of the product about which complaints are made appears to be somewhat confusing. See Table 1

“Component or Part”	Comment
ELECTRICAL SYSTEM	Needs to be broken down further
EQUIPMENT	Who is to know what might come under this category?
EQUIPMENT, ADAPTIVE	Are we talking about, say an adaptive vehicle speed control? If so, should it not come under “VEHICLE SPEED CONTROL”
PARKING BRAKE	Surely the braking function is performed by service brakes when the vehicle is running and by the parking brake when the vehicle is stationary. Whether the braking function is enhanced by air, vacuum, electric or hydraulic means may be important, so the data structure for the braking system needs to reflect this, which it does not do at present.
SERVICE BRAKES	See above comment
SERVICE BRAKES, AIR	See above comment
SERVICE BRAKES, ELECTRIC	See above comment
SERVICE BRAKES, HYDRAULIC	See above comment
STRUCTURE	A category that needs to be broken down further
STEERING	A system that needs to be broken down further
SUSPENSION	A system that needs to be broken down further
UNKNOWN, OR OTHER	Gloriously vague and ambiguous: tends to be used as a catch-all
VEHICLE SPEED CONTROL	Needs to be broken down further
VISIBILITY	Not a “component or part”
TIRES	Surely the tyre is part of the wheel sub-assembly
WHEELS	Surely the wheel assembly should include the tire as a component part

Table 1 Complaint categorization by Component or Part in the NHTSA-ODI Database

I feel reasonably certain that such a complaint categorization could be much more closely related to a well-defined automobile product structure breakdown and be taken to a lower level of detail reasonably easily. Such a “complaints tree” must already exist somewhere. There also needs to be some capability to categorize according to type of fault which is being complained of, in particular, to identify intermittent faults. There are plenty of good precedents here within the automobile industry and outside for the development of cause and effect diagrams and Fault Tree Analysis for building up diagnostic trees

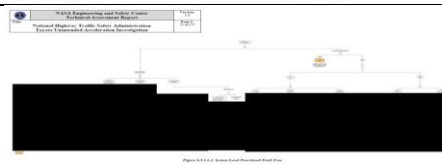
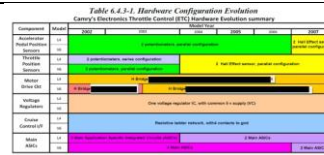
In this this area there is no need to reinvent the wheel and cross-fertilization with other industries, such the aircraft industry, would provide some useful guidance as to developing rules for classification that could form the basis for a complaints system that would be capable of gathering key information about any particular complaint effectively and efficiently. This could be treated as a more or less self-contained pilot project the results of which could be applied later to any early warning system, which clearly has to be closely linked anyway to any complaints system.


9. The harmful and counter-productive effect of redaction on identifying root causes of failure and taking measures to prevent them

Following the Saylor crash in August 2009 and the resulting Congressional hearings on SA early in 2010, NHTSA commissioned (1) the National Aeronautics and Space Administration (NASA) to investigate sudden acceleration in Toyota vehicles fitted with electronic throttles and (2) the NSA to study sudden acceleration in general. About \$3m was budgeted for the two studies in total. The NASA study had limited terms of reference and severe budget and time limitations. Yet the report has been presented as if it was an exhaustive exploration of the subject which, in my opinion, it was not. This paltry sum should be compared with the \$1600 million Toyota MDL settlement, of which \$200million, or thereabouts, went to the MDL lawyers and the \$1200 million fine imposed on Toyota for the concealment of the causes of sudden acceleration by the Department of Justice.

In my opinion, NASA engineers and scientists involved in this investigation did their very best, with the limited time and resources available to them, to carry out a significant pilot project which was deserving of second stage funding, which never materialized. NASA staff, being professionals, undoubtedly burned the midnight oil in order to do the research and write the report against a tight deadline. It is a report upon which others can build. It is a report that stimulates thought amongst other engineers. However, it was heavily redacted, see Fig 5.

- 1. Changes in the throttle motor drive circuit over the years 2002 to 2007 were redacted**
- 2. The System Level Functional Fault Tree was heavily redacted thereby concealing possible fault modes.**



	<p align="center">NASA Engineering and Safety Center Technical Assessment Report</p>	<p>Version: 1.0</p>
<p>Title:</p>	<p align="center">National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation</p>	<p>Page #: 84 of 177</p>

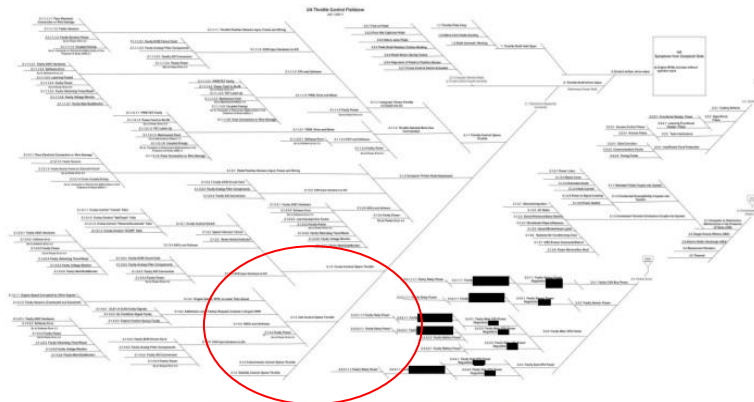



Figure 6.6-1. Fishbone Diagram of Postulated UA Causes

- 3. The possible causes of power error were redacted.**

	<p align="center">NHTSA Engineering and Safety Center Technical Assessment Report</p>	<p align="right">Version 1.0 Page 22 of 34</p>
<p>Title:</p>	<p align="center">National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation - Appendix A</p>	

[illegible]

- #### 4. The software appendix was heavily redacted

Figure 5. Redaction in the 2011 NASA Report into Sudden Acceleration in Toyota Vehicles

This report was paid for with taxpayers' money: therefore, should it not **all** be in the public domain? The redaction of this report, allegedly to "protect" Toyota's commercial interests, destroys much of its value, both to the public and to Toyota, because among other things, redaction **conceals** a number of important the fault modes that the report identifies. In my opinion, public safety interests would have been better served by publishing the **un-redacted** report and thereby stimulate informed technical discussion within and outwith the automobile industry. The following statement escaped the censor's pen:

"Due to system complexityand the many possible electronic hardware and software system interactions, it is not realistic to attempt to 'prove' that the ETCS-I⁵ cannot cause UAs. Today's vehicles are sufficiently complex that no reasonable amount of analysis or testing can prove electronics and software have no errors. Therefore absence of proof that the ETCS-I has caused a UA does not vindicate the system.

Here the NASA investigators were working on the basis that 'absence of proof *is not* proof of absence', as would other competent engineers and scientists if they were engaged in a similar investigation. At the press conference when this report was released US Secretary of State for Transport Ray La Hood said to the contrary:

"We enlisted the best and brightest engineers to study Toyota's electronics systems, and the verdict is in. There is no electronic-based cause for unintended high-speed acceleration in Toyotas. Period."

Why did the Secretary of State say this, and on what scientific basis? Toyota continues to hide behind this governmental exoneration to this day. This affirmation has been taken as gospel truth in other countries, for example in Uganda. There in early 2013 Mrs Jaqueline Usera Nsenga at the gates of her compound experienced a confined space sudden acceleration in her Toyota which ran over her husband, who later died of his injuries. Had Toyota electronics not been exonerated, the possibility of sudden acceleration as a causal factor would not have been dismissed out of hand by the judge and would have been considered as a possible cause of the incident to be weighed against other possible causes. Mrs Uwera Nsenga was tried for murder and was given a 20 year jail sentence⁶.

Following on from the NASA study, the Toyota software was analysed further under the aegis of the Toyota Multi-district Litigation (MDL) by Mr Michael Barr and his team under the most stringent secrecy conditions. This was allegedly to protect Toyota's software "Crown Jewels". However, in my view, this emphasis on security is highly questionable. If Toyota had any significant intellectual property in its software it would be protected by patents and the company would be able to take care of any infringement issue in the patent courts. In any case, the software under investigation in 2011-2012 was for a 2005 MY Camry and had long been superseded.

10 The Bookout v Toyota case and its consequences

In September 2007, a 2005 Camry driven by Jean Bookout sped out of control as she was exiting from an [Oklahoma](#) highway. Bookout couldn't stop the car and it crashed, injuring her and killing her passenger Barbara Schwarz. In October 2013 the Bookout v Toyota case came to trial in Oklahoma. This appears to have been the first Toyota case in which the software/ Electronics in the electronic throttle was on trial. Critical to the eventual verdict in favour of the plaintiffs was the evidence of Mr Michael Barr and his team who built on their work in the Toyota MDL case and examined all 10 million lines of source code for the electronic throttle control of the 2005

⁵ ETCS-I = Electronic Throttle Control System - Intelligent

⁶ [Uganda v Uwera Nsenga](#) 22 September 2014 < <http://www.ulii.org/ug/judgment/high-court/2014/43-0>>

Camry, which was a truly formidable task. Mr Barr's 700+ page expert report provided the basis for his opinions expressed in court. He found some notable deficiencies in the Toyota software that, in his opinion, could explain how the electronic throttle might move to the wide open position without triggering a fault code. He concluded:

- Toyota's electronic throttle control system (ETCS) source code is of unreasonable quality.
- Toyota's source code is defective and contains bugs, including bugs that can cause unintended acceleration (UA).
- Code-quality metrics predict presence of additional bugs.
- Toyota's fail safes are defective and inadequate (referring to them as a *"house of cards" safety architecture*).
- Misbehaviours of Toyota's ETCS are a cause of UA.

The state court jury rejected Toyota's defence of driver error in favour of the plaintiffs case against the software as cause. Since the Bookout verdict Toyota has settled large numbers of claims out of court for undisclosed sums.

Notwithstanding the Bookout verdict, Mr Barr's full 700+ page report, which was the basis for his testimony, remains strictly under lock and key to this day **and even he does not have a copy of his own report**. He signed a nondisclosure agreement and according to him⁷, **the terms of that nondisclosure agreement are also secret**.



Figure 6. The 700 page Barr Report remains under wraps and cannot be discussed

In effect, the shortcomings in safety critical software that Mr Barr identified have been censored and he cannot discuss them with anyone under pain of severe sanctions by the MDL Court in California. This means that **nobody** can learn lessons that might be useful, regarding how not to write software. This is an extraordinary situation, quite unparalleled, in my opinion, in the annals of engineering failure investigations.

Since the tendency is to use increasingly complex software in automobiles it is essential to sort out yesterday's mistakes in order to prevent the potential for even greater mistakes in the future. So long as the Barr report remains under wraps it is not possible to make more than an informed guess as to the software deficiencies that were found.

Toyota makes great play of accepting a DOJ fine of \$1.2billion dollars for concealment of sticky pedals and floor mats and saying sorry. Surely, as a gesture of good faith - an indication that it will never take the

⁷ The design decisions for the XV30 would have been more or less fixed by 1998, including the requirements for the software.

concealment path in the future it, and will put its best endeavours behind implementation of ISO 26262 - it would be appropriate for Toyota to release Dr Barr's report immediately. Not to release the report is, in my view, tantamount to saying that they have every intention of carrying on with acts of concealment concerning safety-critical vehicle electronic control systems wherever and whenever they can get away with it.

Published Engineering Failure Reports allow discussion, if necessary controversy, and at the end of the day, result in improvements that may prevent similar incidents from occurring in the future. Here are some examples where lessons have been learnt from well-documented failure investigations and reports: high pressure boiler explosions in the early steam locomotives, which eventually resulted in design codes for high pressure boilers⁸; the Tay Railway bridge disaster (1879) which revealed a whole catalogue dangerous practices and started the process properly organised strength testing of components for bridge, ship and aircraft construction and led to an understanding of the need to take account of wind loadings; ship disasters, such as the Titanic (1912); The Tacoma Narrows Bridge collapse; the mysterious Comet jetliner crashes in the early 1950s, which were eventually pinned down to metal fatigue; the Rolls Royce RB 211 jet engine failures, identified as due to bird strike on take-off. The list is endless.

My point is that by bringing out failure modes and effects into the open it becomes possible to think of ways and means of avoiding such failures in the future. **So long as failures and the potential failure mechanisms are redacted, the likelihood of further failures occurring, perhaps on a bigger scale, remains.**

When it comes to safety critical electronic control systems, with their heavy reliance on computer software, in most industries it is taken for granted that the design will be subject to **rigorous external audit at the design stage** in accordance with Functional Safety Standard ISO 61508 which, since 2000, has been the norm⁹. The manufacturer has to produce a safety case before the software can be used, say, in a nuclear power station. Not so in the automobile industry where there is no external review or scrutiny whatsoever and in particular not at the design stage. **In my view, as I have suggested earlier, the whole culture of the automobile industry has to change so that it falls into line with other safety critical industries and accepts a measure of independent review as far as its design procedures are concerned.**

It appears that automobile companies, by appealing to the courts on the need to protect their commercial interests, are able to get the backing of the law to conceal the faults in the construction of their software. As a result, engineering and safety communities cannot discuss and consider what lessons may be learnt concerning the writing of safety critical software. This is in my opinion an intolerable and truly disgraceful absurdity, which runs counter to interests of ensuring public safety.

⁸ [Leveson](#)

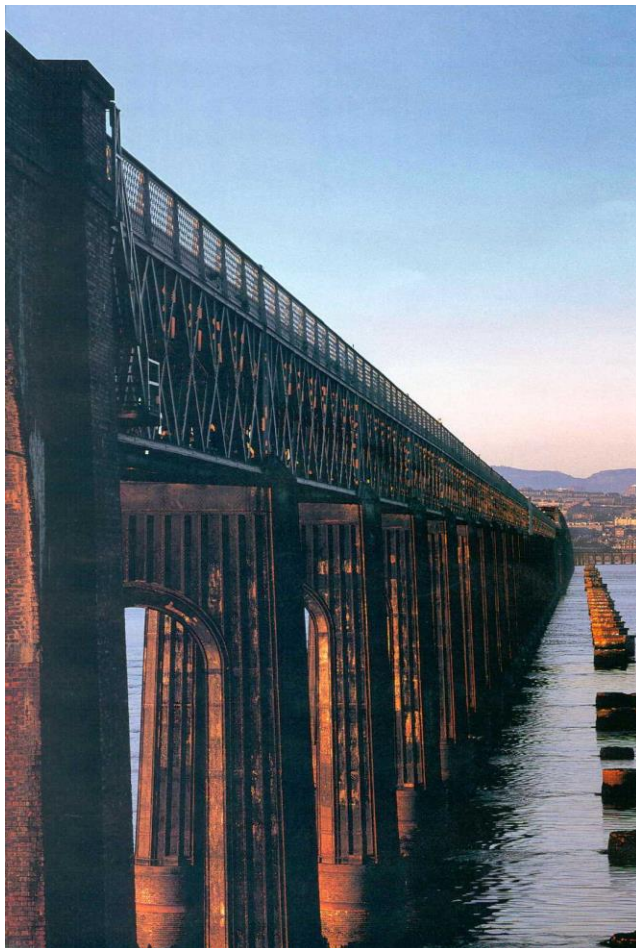
⁹ The first edition of ISO 26262, which is an adaption of IEC 61508 for Automotive Electric and/or Electronic Systems, was published in November 2011. This standard 'addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems, including interaction of these systems'. ISO 26262 has not yet been fully implemented. In practical terms, manufacturers concerned to establish a high level of electronic functional safety should start by building into their electronic throttle designs effective means of automatically reducing or cutting engine power in an emergency that are *totally* independent of the vehicle's own electronic speed control system/ electronic throttle.

NHTSA, for its part, could advance the cause of openness regarding intermittent electronic and software malfunctions considerably - and at very small cost:

- By de-redacting the 2011 NASA report
- By putting pressure on Toyota to release the Barr report as a gesture of good faith and an indication that the Company is starting to take the implications of ISO 26262 seriously.

Antony F. Anderson

Antony Anderson December 6th 2014 Newcastle upon Tyne UK



Tay bridge Disaster December 1879

On the right are the bases of the piers of the original bridge that was blown down in 1879.

A reminder of a major engineering failure.

Left the present bridge which was far more substantial and designed with the benefit of knowledge gained from studying the failure mechanisms at work that caused the original disaster.

Here at low tide the extent of the failure of the original bridge is still a visible reminder to all engineers of the importance of learning from disasters.