Toyota “sticking pedals” recall a smokescreen?

Most of their sudden unintended acceleration problems are almost certainly caused by their vehicles’ electronics

– either by electromagnetic interference (EMI), and/or lead-free soldering, and/or software “bugs”

The professional opinions of EurIng Keith Armstrong CEng FIET SMIEEE, ACGI
www.cherryclough.com, phone/fax: +44 (0)1785 660 247

Version 4.0 2nd April 2010

Contents

1 NHTSA contacted me for advice on EMI and Toyota electronics

The US Government's National Highway Traffic Safety Agency (NHTSA) has wanted to speak to me for some weeks to discuss the EMI implications of Toyota's spate of sudden unintended acceleration incidents. They said they wanted to speak to me because they had no one on their staff with my experience or knowledge of EMI and EMC.

I imagine the fact that I've been presenting IEEE EMC Symposium papers on EMC and Functional Safety since 2001, including one addressed to the auto industry at a symposium in Detroit in 2008, played a part in their decision.

They also said they wanted to speak to my colleague, Dr Antony Anderson (www.antony-anderson.com), a forensic electrical engineer, because they had no one with his knowledge or experience either.

On February 2nd, I spoke for over an hour with two of their senior officers. At the time, I was in Florida as an Expert Witness against the Ford Motor Company (my first ever appearance in court, anywhere, for any reason!) attending a Sudden Unintended Acceleration case as an Expert Witness against the Ford Motor Company. Unfortunately, a confidentiality agreement prevents me from describing what we discussed.

2 CTS pedal replacement could not have saved Mark Saylor and his family

California Highway Patrol officer Mark Saylor and three family members were all killed when their Lexus crashed and burned after a 100+mph race down a highway in San Diego County, on August 28, 2009, see http://suddenacceleration.com/?p=302.

During the incident one of his family phoned 911 and spoke to the emergency services for nearly one minute. You can hear a most distressing recording of the call at http://suddenacceleration.com/?p=431.

It is not credible that a Highway Patrol officer with Mr. Saylor's nineteen years of experience would have pressed the wrong pedal, or been unable to deal with a gas pedal that got stuck on a ridge in the floor mat, or was a bit sticky, for over a minute with a car full of passengers. And CTS, whose alleged "sticky pedals" are being replaced in the current Toyota recall, recently said "*CTS wishes to clarify that it does not, and has never made, any accelerator pedals for Lexus vehicles and that CTS also has no accelerator pedals in Toyota vehicles prior to model year 2005.*"(see:
www.google.com/hostednews/afp/article/ALeqM5jXlnWY76DKARDE459OFtAWoYEZdA)

It was Mark Saylor's terrible fate that started this current media furor over runaway Toyotas, which started off as a "Toyota Sudden Acceleration" story. But I note that over recent weeks it has morphed into a "Toyota Sticking Pedals" media story, with terrible accidents like Mark Saylor's played down - as if a floor mat or sticky CTS gas pedal could somehow have been the cause of his death along with three members of his family.

3 It is difficult/impossible to stop a runaway vehicle with the brakes

Tests performed by the motor industry, by the Japanese Government, and for the US Government, including NHTSA's 2007 tests on a Lexus ES-350 [11], all show that it is very difficult indeed to stop a runaway vehicle with the brakes – and may be impossible for some people. Even if you do manage to do it, the stopping distance is enormous. This assumes that the

brake pedal is pressed only the once, and is kept firmly pressed down until the car stops, and is not "pumped."

[11] shows that with its throttle forced wide open, a brake pressure of 150 pounds – 5 times more than the usual 30 pounds) was required to stop a vehicle from a certain speed. The report also shows that it took 1,000 feet to stop – 5 times more than the usual 200 feet from that speed. And that was with drivers who were *expecting* the sudden increase in engine revs and so had no "startlement" delay.

Many drivers don't even weigh as much as 150 pounds, but even someone of that weight or more would find themselves having to pull up very hard on the steering wheel, using both hands, to try to get enough brake pressure even with both feet on the brake pedal. Now, imagine trying to steer your car for 1000 feet whilst pulling on the steering wheel like that, steering around other traffic, people, street furniture and all the rest. Most likely, violent steering maneuvers will be required, but you can hardly turn the wheel more than half a turn each way because to do so would mean taking a hand off the steering wheel and so pressing less hard on the brake.

Now imagine trying to spare a hand from the steering wheel for the 3 seconds of *continuous* pressure on the 'Start' button, which is the only way to turn off the ignition on the Lexus [11]. Or trying to force the gear lever into Neutral. Whilst also doing all of the above.

Clearly, it is very difficult, and probably impossible for many drivers, to safely bring a vehicle to a stop on normal roads, if some malfunction has forced the throttle wide open.

Also, many people have been taught that if the brakes don't stop the car quickly enough, pumping can help increase brake pressure. This is the wrong approach when the engine is high-revving because in this condition it does not provide much vacuum for the brake booster. If you press the brake pedal more than just the once when the engine is revving flat out - you lose the brake boost from its vacuum servo and braking effectiveness is actually lost.

Many people who suffer sudden acceleration accidents in many makes of vehicles (most automakers have – or have had – this problem, as NHTSA's database shows) report that their brake pedal went very hard – indicating a loss of vacuum boost, and consequently less effective braking.

4 EMI generally leaves no trace of a "defect" after an incident

4.1 Why no "defect" can be found afterwards

Switch on a light. Then switch it off. Now prove that the light was ever switched on. You can't do it – the electricity that flowed in the circuit leaves no trace. The light can only be either on or off, but electronic circuits have many different ways in which they can operate, and just like the light, none of them leave any trace in their circuits afterwards.

Digital circuits (e.g. microprocessors running software) have an almost unlimited number of possible modes of operation, only a few of which are desirable modes – modes that we *want* to occur. As electronic design engineers we are used to having to improve our designs so that they behave the way we want them to, operating in only the modes that we want at the appropriate times, with sufficient reliability for the application they are intended for.

Where correct operation at the appropriate time is important for ensuring that safety risks are low enough, we find that the reliability of ordinary electronic devices and circuits, and the way they are designed, is not good enough. One of the reasons for this is the possibility that EMI of one sort or another, or several types of EMI occurring at the same time, might cause errors in

operation to exceed tolerable limits, or cause the operational mode to change to one that is undesirable at that time.

Special design measures, maybe special components, are required where electronic circuits of any kind are used in applications where, if they suffer errors or misoperation, the resulting safety risks would be too high.

Because our history first went through mechanical technologies, then hydraulic, pneumatic and electromechanical, our institutions have become used to the idea that if a thing fails to work as intended, then there must be some damage or "fault" that caused this to happen, and the damage or fault can be discovered by careful inspection, even after an accident.

We are all familiar, from media reports, of how after an air crash, investigators collect all the bits and pieces they can found and reassemble the aircraft, to try to identify what it was that caused the accident. They are highly-skilled in discriminating between the damage caused by the accident itself, and the damage or fault that caused it.

But If a light is turned on when it is supposed to be off, it doesn't suffer any damage. In exactly the same way, when an electronic circuit operates in the wrong way, or at the wrong time, it doesn't suffer any damage either, and – like the light – once it has been switched off there is no trace of its former incorrect behaviour.

When electronic circuits, or the software or firmware that runs on them performs one of its normal operations at the wrong time, for example turning the aircraft rudder to the right, instead of to the left; or when it performs a correct operation but with an error - for example setting the rudder angle to 60 degrees instead of 6, the electronic circuit suffers no more stress than if it was behaving normally. As far as it is concerned, it is performing a normal operation.

So the traditional approach to accident investigation, post-accident reconstruction, which has worked so well for many decades, fails us when we have to deal with electronic errors or misoperations.

We tend to talk about an accident suffered by a computer-controlled vehicle (such as a modern aircraft or automobile) being able to be caused by a "fault" in the controlling electronics, but this is really an inappropriate word in this context. The word "fault" tends to imply – because of our history – something that can be discovered after an accident. But accidents can be caused by errors or misoperations in the controlling electronics, which cannot be discovered afterwards.

Another word often used in connection with electronics is "malfunction" – implying a "bad function" or incorrect operation. Once again, like the word 'fault', this word can mislead us, because it can be assumed to imply some kind of fault that would leave a trace. However, a malfunction in an electronic circuit can be nothing more than it performing one of its normal functions, but at an inappropriate time, or with a larger than usual error.

For these reasons I prefer to use the term "misoperation", because it carries a lower expectation of being able to find the cause of the accident after the event.

Of course, electronic faults can occur, such as (for example) short-circuits or open-circuits due to poor soldering, or poor quality components that fail, and these can generally be discovered after an accident. However, it has to be said that this can be very difficult with a poor quality connection that creates an intermittent contact – the shock of the impact or the activities of the investigators can be enough to temporarily restore the connection to an apparently good state, which may last for weeks, months, even years before becoming bad again. Intermittent connections, and the difficulty of discovering them, is a problem that has plagued the automobile industry ever since electricity was used in vehicles, and the very small voltages and very weak currents in modern electronics only makes the situation worse.

Malfunctions in electronic circuits can be caused by electromagnetic interference (EMI), and this is explained more fully in Annex B of the IET's 2008 Guide on EMC for Functional Safety [1].

Some types of EMI, like direct lightning strike, have sufficient energy to cause actual damage, and as a result are relatively easy to diagnose after the fact. Electrostatic discharge can also sometimes cause damage, but an electron microscope is usually needed to spot it. Most types of EMI do not have sufficient energy to cause actual damage. They are very weak and do no more than distort or otherwise confuse the electronic signals in a circuit, causing it to suffer from errors or malfunctions in the operation of its hardware, software or firmware.

Many electronic circuits will eventually recover from their errors or malfunctions when the EMI is removed. Analogue circuits can recover quite quickly, whereas digital microprocessors running software or firmware might have to wait until they are reset by a "watchdog" circuit, which in some cases might take several seconds, although careful design is required to make sure that watchdogs will recover from all foreseeable situations. Digital "state machines," and electromechanical "relay logic" can remain in an incorrect state until reset manually.

If an electronic malfunction does not disappear of its own accord or due to circuit operation, it might be possible to detect it after an accident as long as the ignition is not turned off. But one of the first things people do after an accident is turn off the ignition, so such evidence is immediately lost. Police and other emergency services/first responders might even disconnect the battery to help prevent fires from occurring in damaged vehicles, similarly erasing all evidence of the malfunction.

Even if the vehicle in question was left running with its engine screaming away, it would take quite some time to get the appropriately skilled people and their electronic test gear to the site, by which time the vehicle may have run out of fuel or the engine may have overheated and failed for some reason due to its unusual stress, or the consequences of damage in the accident. Even if you could get an "emergency electronic response team" to the site of an uncontrollably revving vehicle, it is often impossible for them to access the points in the circuits that they need to attach their probes to, without dismantling a module. And dismantling might require the module to be unplugged and so lose its power.

4.2 Technology outpaces the institutions we rely upon to protect us

In the US, the legal system – upon which we rely to protect us from manufacturers who have become over-zealous in the pursuit of profit at any cost (that is, any cost to us) – has great difficulty with the idea that the "fault" that caused an accident is not discoverable afterwards.

This also appears to be a problem suffered by NHTSA, whose accident investigators expect to be able to find the "fault" that caused the accident, after it has occurred.

But I suppose it is only be expected – after all, it is barely 30 years since the first use of electronics in controlling a safety-related vehicle system (cruise controls), and the law and government agencies don't appear to be able to change very quickly. It wasn't helped, of course, by at least one major vehicle manufacturer classifying their cruise controls as driver conveniences, rather than safety-related systems. The same manufacturer classified all safety issues as "driveability".

This slow pace of change in the institutions we rely on to protect us in the USA, presents great problems now, and worse problems in the future as technology continues to change more rapidly still.

In Europe, the pace of change of the law and government agencies is just as slow as in the USA. But manufacturers over there have traditionally accepted greater government interference in what

they can and can't do. This is usually manifested as technical regulations, or technical standards, that manufacturers are required by law to comply with.

In the case of a vehicle accident, the idea in Europe is that investigators will go through not only the vehicle in question, but also over its design and the quality of its manufacture. If anything is found not to comply with the technical regulations or standards, this makes it difficult for the manufacturer to claim that his vehicle was "safe enough".

Consider the results of these two approaches:

a) In the USA, plaintiff's have to try to prove that the vehicle was not as safe as the state of the art. Their lawyers have to try to discover whatever they can about the vehicle's design and manufacture, and, by "reverse-engineering", discover the "defect".

   The auto manufacturers claim that their vehicles are all designed and manufactured fully in accordance with the state of the art in safety, then make it very difficult for plaintiff's lawyers to 'discover' anything.

   For example, one auto maker classified all field service reports of malfunctioning cruise controls as non-safety-related, and kept them for one year before shredding. (Safety related complaints had by law to be kept for very much longer.) When NHTSA asked them for copies of all field service reports concerning problems with cruise controls, they said (quite honestly) that they only had a few. The hundreds they had shredded were never revealed to the government.

   Another practice that is common in US manufacturers of all kinds of products, not just cars, is to delete or shred all of the safety design information, once the product is in volume-manufacture.

   The system encourages manufacturers to be secretive about their product's safety – to make grandiose claims that their product's are "perfectly safe" – which everyone know is impossible anyway – and then hide behind bluster rather than back their claims up with hard data.

   If vehicles really were as safe as the state of the art when they are designed, what is it that their manufacturers are trying to hide?

b) In Europe, if a product manufacturer can't provide documents showing that they applied the state of the art in safety during design and manufacture, the courts assume they didn't do the work.

   So European manufacturers keep their safety design documents in a safe place, in case they ever have to prove that they actually did do what they said they did, on safety. Since they always apply the state of the art in safety anyway, just as they claim, therefore they have nothing to hide.

   This system encourages manufacturers to be open about their safety design, to provide hard data to convince the courts that they really did do a good job of safety design and Quality Control in manufacture.

   The aim of this approach is to try to redress the hugely unequal balance of power between a large corporation, such as an international auto maker, and a private individual. It is intended to make it more likely that an individual will get justice when they can't afford to put up millions of dollars for several years (or find someone else to put up such large amounts of money for them).

As a private individual, imagine trying to sue a major international auto maker for the death of a relative. Which system is likely to give you the fairest chance – the best chance of getting any sort of justice?

4.3 "Latch-up" as a possible cause

A class of rather more serious electronic device malfunctions is called "latch-up," and makes an entire integrated circuit (IC) "seize up", as if catatonic, with all of its outputs frozen at full-scale (either high or low.)

Latch-up is caused by any pin of an IC being driven to more than a volt or so beyond its positive or negative DC power supplies, either by overvoltage or undervoltage transients. This can happen due to conducted, induced or radiated noise coupling, e.g. from the inductive flyback of switched loads (spikes), or electrostatic discharge (ESD.) Interestingly, ICs are more susceptible to latch-up when they are hot, and/or when exposed to ionizing radiation.

The pins of microprocessors in an automobile are exposed to spikes and ESD all the time, in particular spikes from the ignition system. EMC tests done by automakers, and/or their suppliers, should ensure that ICs are normally immune to those EM phenomena in a vehicle and so don't latch up (but see item 5 below for the limitations of testing). But when a secondary cosmic ray shower reaches the earth's surface the additional radiation might be sufficient to allow an ignition system spike to cause the microprocessor to latch-up.

I haven't yet found data for the probability density function for the intensity of cosmic radiation at the earth's surface, so can't estimate whether it ties up with the number of runaway Toyotas.

The only thing that will recover an IC from a latched-up state is to turn its electrical power supply off. When turned back on again, it performs as normal again. Latch-up is a problem for all types of ICs, whether analogue or digital, and of course when a digital processor is latched-up, its software or firmware cannot run at all, so any recovery techniques they have designed into them cannot work.

During a latch-up, the IC's electrical power consumption is only limited by its external power supply circuit. If this has a low impedance and can supply a high current, the IC can overheat and suffer obvious damage as a result. The electrical supply in an automobile is nominally 12Vdc (actually, closer to 14V in normal driving) but most ICs used in auto electronics have to be operated at lower voltages, such as 8V for early analogue cruise controls (e.g. using the Intersil CA 3228E) or 3.3V for a modern digital microprocessor.

While the vehicle battery is capable of sourcing hundreds of Amps, the voltage reduction circuits that power the electronics from the vehicle's 12V supply have a limited current rating and often aren't capable of delivering enough power to a latched-up IC to allow it to heat up by enough to cause damage, or even obvious discoloration. So, once again, we find that the malfunction leaves no evidence after the fact.

Latch-up used to be a very serious problem when ICs were first used in automobiles in the 1980s, but over the years the semiconductor industry has become better at designing protection into its ICs. However, like all EMI issues, it is impossible to provide 100% guaranteed protection against latch-up, especially when "showers" of secondary cosmic radiation are taken into account.

Toyota use two microprocessors in their engine control unit (ECU) an attempt at redundancy, but – as I will discuss in more detail later – if they use the same technology, and are exposed to the same EMI, it should be assumed that they will both suffer similar errors, misoperations or failures, at the same time.

The two microprocessors in the ECU will share the same power supplies, and may even share some input signals. So over/undervoltages on those common connections could make them both latch-up at the same time.

But it is not necessary for the microprocessors to latch-up to cause a sudden uncontrolled acceleration. The transducers that control the fuel injection, throttle valve setting and ignition timing are not driven directly by the microprocessors – their signal are too weak for that. Instead, the microprocessors send control signals to other ICs, which amplify their weak signals up to the power levels adequate to power the mechanical and hydraulic parts, and the spark ignition coils.

Ronald A Belt (mrbelt@voyager.net) recently reminded me that these "driver" ICs can latch up too, and since they are connected directly to battery power and to long cables, they can be more exposed to the over/undervoltage transients that can cause latch-up, than the microprocessors. Depending on the circuit design, latch-up of these ICs could result in sudden uncontrolled acceleration.

4.4 What kind of errors and misoperations can occur?

When vehicle electronics have control of the butterfly valve in the throttle, as all cruise control and throttle-by-wire systems do, a misoperation in their hardware or firmware can cause the butterfly valve to take on an uncommanded setting (i.e. not one that the driver commanded by his use of the vehicle's controls).

It might close shut, oscillate, stick fast at some angle, or open wide.

In a recent case in Australia (concerning a Ford rather than a Toyota), what appears to have happened is that the cruise control stuck on at 80kph, and the driver could not switch it off or change its speed setting. See: www.theage.com.au/national/no-fault-in-cruisecontrol-terror-car-20100107-lwdd.html?autostart=1).

All of these possibilities have safety consequences for control of the vehicle, but the scariest of them all is the wide-open-throttle. This is the one that historically has caused the most accidents, injuries and deaths (see www.suddenacceleration.com and www.antonyanderson.com/cruise/cruise.htm).

It only takes a second or two of unexpected full throttle to cause a potentially fatal accident, so a momentary electronic malfunction from which the vehicle's electronics automatically recovers, can still cause a serious accident and vanish without leaving a trace.

4.5 "Black Box" data recorders

As far as I am aware, the "Black Box" data recorders that provide a record of vehicle operation are not totally independent from the vehicle's electronic circuits. Rather than using their own sensors, which would add significantly to vehicle cost, they record signals taken from the vehicle's existing electronics.

So, for example, if the vehicle's circuits were interfered with and as a result "believed" that a full throttle had been commanded by the driver, the data recorder would show that the driver had pressed hard on the gas pedal whereas an independent sensor on the gas pedal would show a different result.

But modern gas pedals themselves are complex electronic devices, quite capable of being interfered with themselves and giving an incorrect output to the engine's electronic control system. So even if a black box data recorder used an independent sensor for gas pedal position,

if that sensor used the same technology as the one sending the signal to the engine control system, it could well be interfered with in the same way, giving the same false output.

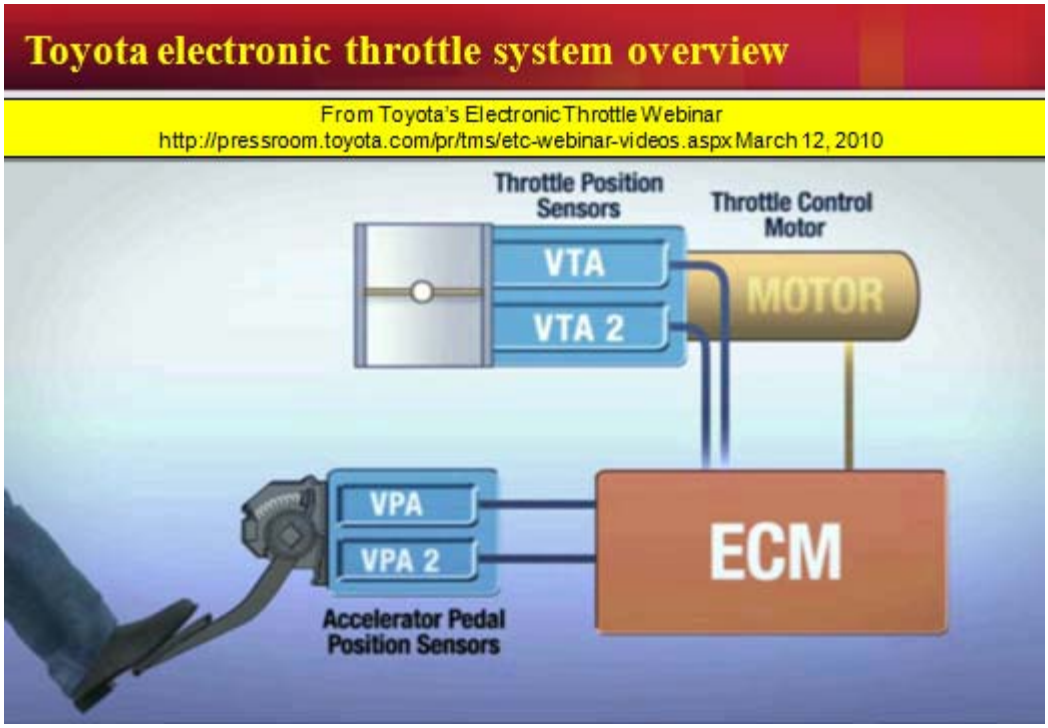
4.6 Redundancy

A common way of improving the reliability of electronic circuits is to use "redundancy," but if the redundant or "parallel" devices or circuits use the same technology, in either the hardware or the software, then they can respond to EMI in the same way at the same time, making the redundancy technique ineffective. For this reason, EMI is known in safety engineering as a "common cause problem".

To be effective, redundant "channels" need to use different software languages and different hardware (especially different types of microprocessors).

This was well-known by safety engineers in the 1990s, and appeared in an international safety standard in 2000: IEC 61508:2000, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems", IEC basic safety publication, from http://webstore.iec.ch.

Toyota's "Electronic Throttle Webinar" (http://pressroom.toyota.com/pr/tms/etc-webinar-videos.aspx) shows the use *so-called* "dual-redundant" systems for throttle control in the gas pedal position sensors, throttle valve position sensors and throttle control microprocessors, all of them using (it claims) identical technologies. See the figure below.

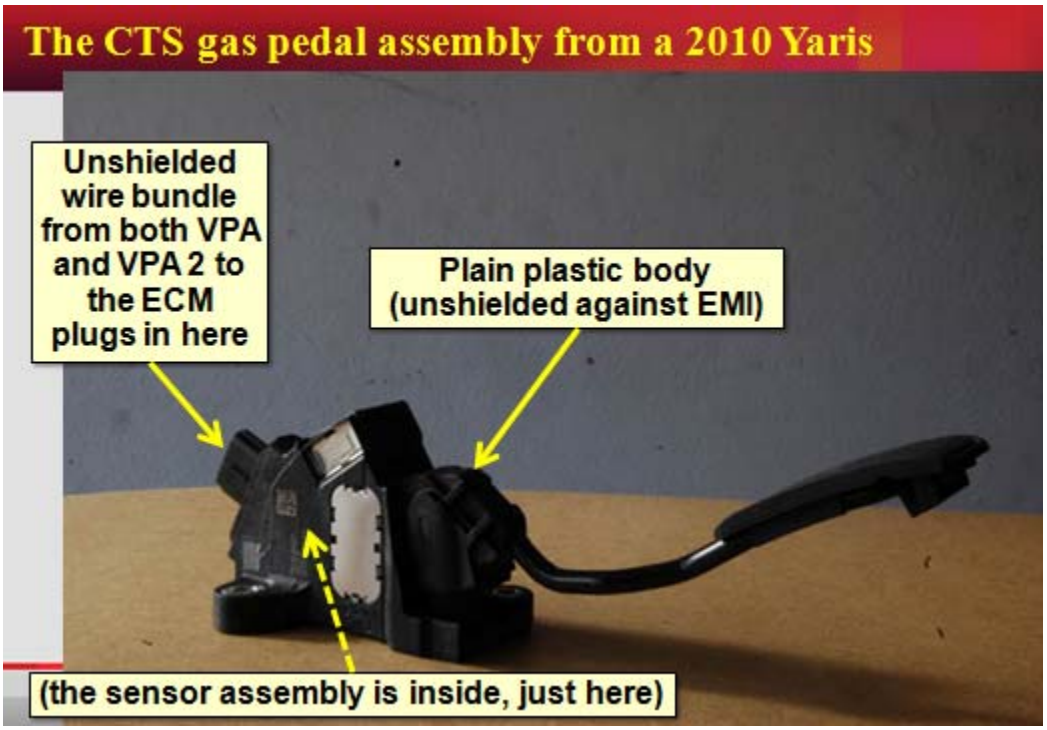


The webinar claims this means that failure for any reason (including EMI) will be detected, but we know that because the redundant systems use identical technologies (as the webinar says), "common cause" errors or failure modes not protected from.

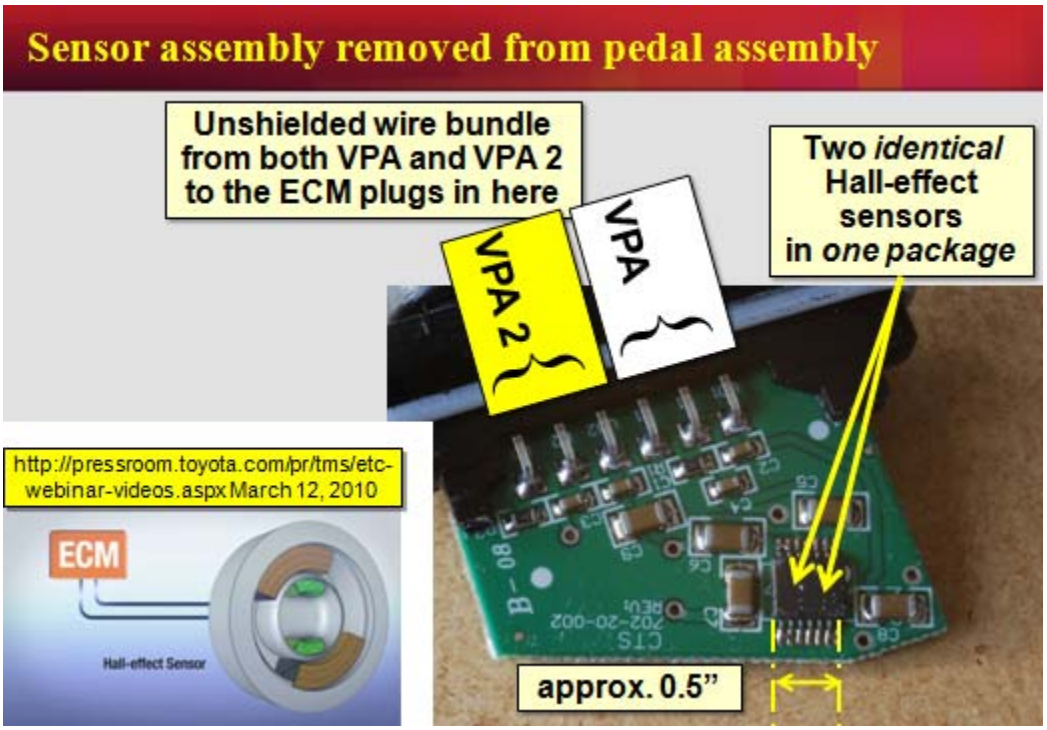
This is easily proven by simply holding a bar magnet close to the gas pedal sensor, causing engine speed to change. This is clear evidence that their so-called redundant system cannot detect a "common-cause" error, such as EMI. NHTSA noticed in 2008, see [11], that placing a magnet near to the gas pedal sensors or to the throttle valve position sensors could cause the

engine speed to rise by 1000rpm, but have apparently failed to see the significance of this in terms of safety.

The figure below shows the CTS gas pedal assembly from a 2010 Yaris.



The next figure shows the *so-called* dual redundant pedal position sensor assembly removed from the above gas pedal assembly, with VPA and VPA 2 indicated.



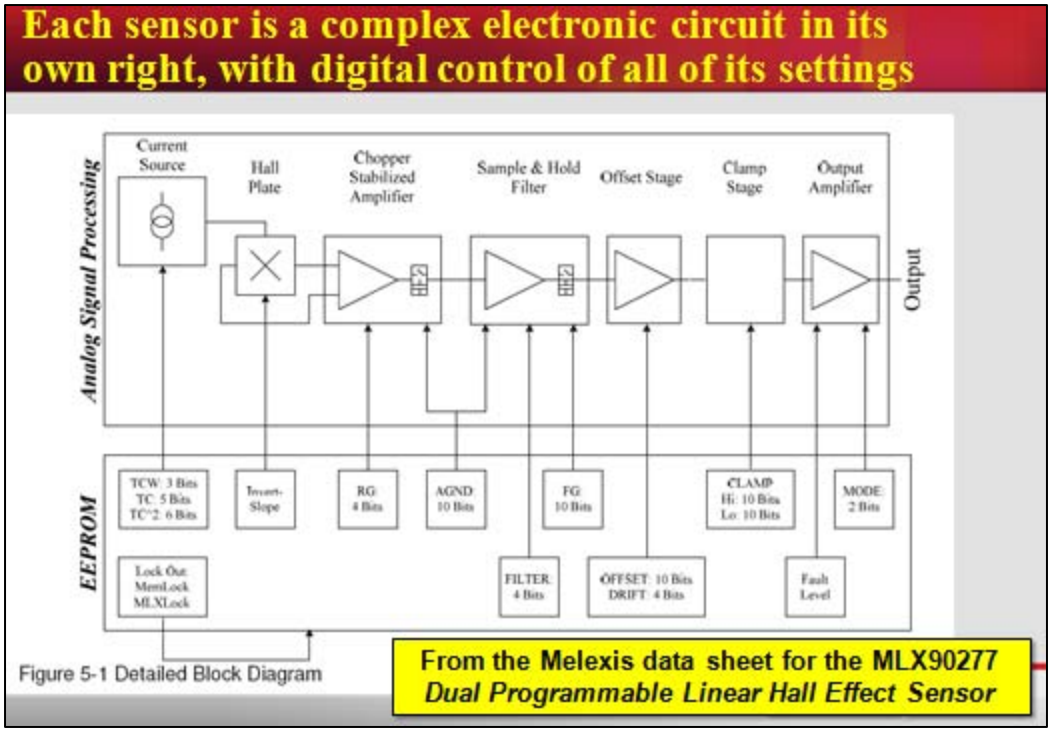
Notice, in the photograph above, that there is only one sensor component. In fact, it has two identical silicon chips embedded within it, so it is really two sensors, but packaged as they are it would be almost impossible for them not to perfectly share almost every aspect of their environment – EMI, temperature, magnetic fields, poor soldering in manufacture, vibration, condensation, etc.

It is almost as if Toyota's designers had gone out of their way to ensure that their *so-called* redundant gas pedal position-sensing system would fail to provide any safety benefits when exposed to EMI.

But we must not blame Toyota's designers too much (although they are to blame), because it seems to be commonplace amongst automakers to use identical technologies in their so-called redunndant systems.

At least, this was what Melexis must have thought when they designed and made their MLX90277 hall-effect sensor IC, the one that is used in the Yaris pedal photographed above – their data sheet [12] makes a feature of how it fits two identical but independent silicon chips in the same IC package!

Any knowledgeable electronic system safety engineer in any other industry, would have run a mile rather than use such an IC in a redundant system, even as long ago as 2000. But not in the auto industry even by 2010, apparently!



The figure above, taken from [12], shows that each hall-effect sensor in the MLX90277 IC is a complex electronic circuit in its own right, with digital control of all of its settings. This means that it is very vulnerable to errors and misoperation as the result of EMI. Yet it is not housed in a shielded gas pedal assembly. The only protection it has against EMI is a few shunt-filtering capacitors mounted on the PCB, and these are vulnerable to dry or cracked solder joints (see later).

System safety experts (at least, those working outside the auto industry) have known since the early 1990s that "diverse technology" is required, if redundant electronic systems are to be effective in reducing safety risks for the hardware (e.g. sensors, microprocessors), and for the software. Otherwise errors or malfunctions caused by EMI and software bugs will have the same effect on each system at the same time.

When errors or malfunctions affect all the redundant systems the same way at the same time, the safety risks are identical to just one system on its own. Redundancy has increased the cost, but made no improvement in safety.

But Toyota's electronic throttle webinar (March 12, 2010) and the Yaris pedal shown above, show the use of identical technologies in their so-called redundant systems giving *the impression* of being more reliable, unjustifiably increasing a designer's confidence.

The need for diverse hardware and software technologies in redundant systems was published in 2000 in the most important international standard on the safety of electronic systems: IEC 61508 [2] so why don't automakers appear to understand this, ten years later?

The references to using diverse technologies in redundant systems are in IEC 61508-7, clause B.1.4 "Diverse hardware" and clause C.3.5 "Software diversity (diverse programming)", both quoted below.

> **B.1.4 Diverse hardware**
>
> NOTE This technique/measure is referenced in Tables A.15, A.16 and A.18 of IEC 61508-2.
>
> **Aim:** To detect systematic failures during operation of the EUC, using diverse components with different rates and types of failures.
>
> **Description:** Different types of components are used for the diverse channels of a safety related system. This reduces the probability of common cause failures (for example overvoltage, electromagnetic interference), and increases the probability of detecting such failures.
> Existence of different means of performing a required function, for example different physical principles, offer other ways of solving the same problem. There are several types of diversity. Functional diversity employs the use of different approaches to achieve the same result.
>
> **Reference :**
>
> *Guidelines for Safe Automation of Chemical Processes*, CCPS, AIChE, New York, 1993, ISBN-10: 0-8169-0554-1, ISBN-13: 978-0-8169-0554-6
>
> **C.3.5 Software diversity (diverse programming)**
>
> NOTE This technique/measure is referenced in Table A.2 of IEC 61508-3.
>
> **Aim:** Detect and mask residual software design and implementation faults during execution of a program, in order to prevent safety critical failures of the system, and to continue operation for high reliability.
>
> **Description:** In diverse programming a given program specification is designed and implemented N times in different ways. The same input values are given to the N versions, and the results produced by the N versions are compared. If the result is considered to be valid, the result is transmitted to the computer outputs.

An essential requirement is that the N versions be independent of each other in some sense, so that they do not all fail simultaneously due to the same cause. In practice it may be very difficult to achieve and to demonstrate the version independence that is the foundation of the N-version approach.

The N versions can run in parallel on separate computers, alternatively all versions can be run on the same computer and the results subjected to an internal vote. Different voting strategies can be used on the N versions, depending on the application requirements, as follows.

– If the system has a safe state, then it is feasible to demand complete agreement (all N agree) otherwise an output value is used that will cause the system to reach the safe state. For simple trip systems the vote can be biased in the safe direction. In this case the safe action would be to trip if either version demanded a trip. This approach typically uses only two versions (N=2).

– For systems with no safe state, majority voting strategies can be employed. For cases where there is no collective agreement, probabilistic approaches can be used in order to maximise the chance of selecting the correct value, for example, taking the middle value, temporary freezing of outputs until agreement returns, etc.

This technique does not eliminate residual software design faults, nor does it avoid errors in the interpretation of the specification, but it provides a measure to detect and mask before they can affect safety.

References:

Dependable Computing: From Concepts to Design Diversity. A. Avizienis and J. C. Laprie, Proc. IEEE 74 (5), May 1986.

A Theoretical Basis for the Analysis of Multi-version Software subject to Co-incident Failures. D. E. Eckhardt and L. D. Lee, IEEE Trans SE-11 (12), 1985.

Computers can now perform vital safety functions safely. Otto Berg von Linde, Railway Gazette International, Vol. 135, No. 11, 1979.

The 2010 FDIS for Edition 2 of IEC 61508-7, uses the following references instead for C.3.5:

Modelling software design diversity – a review, B. Littlewood, P. Popov, L. Strigini. ACM Computing Surveys, vol 33, no 2, 2001

The N-Version Approach to Fault-Tolerant Software, A.Avizienis, IEEE Transactions on Software Engineering, vol. SE-11, no. 12 pp.1491-1501, 1985

An experimental evaluation of the assumption of independence in multi-version programming, J.C. Knight, N.G. Leveson. IEEE Transactions on Software Engineering, vol. SE-12, no 1, 1986

In Search of Effective Diversity: a Six Language Study of Fault-Tolerant Flight Control Software. A. Avizienis, M. R. Lyu and W. Schutz. 18th Symposium on Fault-Tolerant Computing, Tokyo, Japan, 27-30 June 1988, IEEE Computer Society Press, 1988, ISBN 0-8186-0867-6

Also: paragraph 54 (page 12) of “The Tolerability of Risk from Nuclear Power Stations”, The UK Health & Safety Executive, 1992, www.hse.gov.uk/nuclear/tolerability.pdf, says:

54 Redundancy will not, generally, provide protection against inherent design faults, which would simply repeat themselves in every affected component. One way of tackling this is to provide back-up via dissimilar components, i.e. ones that have been designed independently; this approach is called 'design diversity'.

For simple devices this can be very effective, since the versions would almost certainly fail independently of one another. When the task to be carried out is a complex one, however, it may only provide fairly modest reduction of risk.

For example, experiments on diverse computer software suggest that there is a tendency for different designers, independently tackling the same problem, sometimes to make similar mistakes. If this happens, there will be a possibility for some of the faults to be present in all versions, thus creating a chance that these will fail simultaneously in certain circumstances.

4.7 Lack of evidence proves nothing

Just yesterday, I saw in the daily news an automobile manufacturer stating, "We can find no evidence that EMI is a cause of sudden acceleration, therefore EMI cannot be the cause of it." I suspect that all auto manufacturers have used this logically unsound statement over the last 30+ years, Toyota being the latest.

But *of course* we would expect EMI to leave no traces of its passing. Any competent EMC design engineer knows this, including those who work for the auto manufacturers themselves.

This bankrupt argument is still being used today because it can persuade people who don't realize that it is logically incorrect. This is why it is a favorite of politicians and bureaucrats.

For more on this, read my article: "Absence of proof is *not* proof of absence," EMC Journal, Issue 78, September 1998, from the archives at www.theemcjournal.com.

5 It is impossible to prove, by testing alone, that electronics are reliable enough for safety-critical systems such as throttle control

Making millions of vehicles as safe as people expect means reliability of safety systems like engine speed control must be in the parts-per-million-per-year, or less. Ask yourself how often during each year you are prepared to accept that your car brakes or steering will not work, or your engine will run out of control at full throttle. Like most people, you probably answer: *never!*

However, since it is impossible to make products perfectly safe, we must expect that such problems will occur from time to time. We would hope that they don't occur too often and that the automobile designer has reduced the risks of such events so that the risk of death to a driver, passengers or third parties is close to or less than the average risk of dying that we all face as a matter of course (about 1 chance in a million each year for the UK.)

Assuming a vehicle is driven one hour each day, six days each week, every week of the year, this means it is driven for 312 hours a year. Combining this with our target death rate of one in a million each year, this means that our safety-critical vehicle electronics must not fail in such a way as to cause a death at the rate of about $3.2 \cdot 10^{-9}$ per hour's driving. To put it another way, the Mean Time To Failure (MTTF) that causes a death should be 312 million hours of driving, about once in every 35,600 years for a single vehicle driven continuously, 24/7.

Since this is an average calculation, if we were testing to prove reliability, we would need to amass at least 50,000 vehicle-years of continuous testing to begin to have confidence that our design really was in the right ballpark of safety. To actually achieve good confidence in the safety

of our design, we would probably test several examples of vehicles, say ten, continuously for at least 5,000 years each.

According to official NHTSA figures, about 1% of *officially recorded* sudden unintended acceleration events result in a death. So if we assume that only 1% of electronic malfunctions that cause full-throttle malfunctions result in a death, we might feel that we could increase our likelihood of sudden accelerations to $3.2 \cdot 10^{-7}$ per hour of driving, equivalent to an MTTF of 3.12 million hours, which we could get a handle on by testing 10 vehicles continuously for only about 500 years, or 100 vehicles continuously for 50 years each.

Given the time scales over which new models of vehicles are produced, let's assume that the most time that could be allowed for safety testing of the complete, finished vehicle is 6 months. To prove the reliability of our electronics against full-throttle malfunctions we would have to test 10,000 vehicles continuously over that period.

Remember, this assumes that we are allowing vehicles to roar away at full throttle at a rate that is 100 times greater than the risk of dying as a result. Some people might find this idea objectionable, and want a lower rate of full-throttle malfunctions. After all, some of the 99% of sudden acceleration incidents that do not result in a death, will result in injuries of various severities and/or property damage. And those who have no injury, death or damage will still be very frightened and possibly have long-lasting psychological effects.

Of course, the above is a very simplistic analysis and many holes could be poked in it. One hole is that it is estimated that only about 10% of sudden unintended accelerations are ever recognized and reported as such. If a car goes out of control and crashes, killing the driver, who is to say how or why it happened?

For example, in Australia, it is normal for the auto insurance companies to pay out less in the case of an accident that only involved a single vehicle. The assumption is that the driver is always in control of their vehicle, and if it goes out of control it must be the driver's fault, deserving less compensation.

The point I am trying to make here is that the electronic reliability that is required to achieve vehicle safety is much higher than can possibly be proved by any conceivable test plan.

The Institution of Engineering and Technology (London, UK) published its "Position Statement" on "Computer-based Safety-critical Systems" in October 2009 [4]. Obviously, it is aimed at industrial and aviation uses of computers, but of course exactly the same analysis and conclusions apply to computers used in safety-critical computers (e.g. engine management) in automobiles.

Amongst other things, it says:

> "Computer systems lack this continuous behaviour so that, in general, a successful set of tests provides little or no information about how the system would behave in circumstances that differ, even slightly, from the test conditions."

In other words: any amount of testing provides little/no confidence that a throttle controlled by a computer will operate safely.

> "It is generally impractical to rely only on test-based evidence in advance of putting a system into widespread service that the overall probability of failure will be less than 1/100,000 per hour with 99% confidence..."

This is saying that when you need to be very confident that the failure rate of your engine management computer is less than 1/100,000 per hour, no practical amount of testing can ever give you the confidence you need.

Prof. Nancy Leveson says, in [7]:

> "*We no longer have the luxury of carefully testing systems and designs to understand all the potential behaviors and risks before commercial or scientific use*."

It is possible to use one or more microprocessor-based system to act as a safety system for another microprocessor-based system, and this is done in the aviation industry for flight-critical controls. Interestingly, the complexity of the software that pilots use to fly-by-wire a modern jumbo jet is at least ten, maybe a hundred times less than the software used to control a modern automobile [5].

When using such high-technology as a backup system, we face the same problem as the original system – it is too complex to prove that it is safe enough, especially as regards EMI. So instead they acknowledge that the software and the hardware will have problems, and instead reduce them by duplication, triplication, or more so-called "redundant" channels.

But, because EMI causes the same technology to tend to fail in the same way at the same time, and because a software bug will appear under the same conditions each time, simply duplicating a microprocessor system does nothing to protect against these problems. Such duplication will help protect against the effects of random faults – but EMI and software bugs are not random.

It is instructive to learn how modern airlines design their fly-by-wire control systems. Back in the early 1990s I attended a presentation on this at the IEE (as it was then, now the IET) in Savoy Place, London, given by a British Aerospace engineer working on designing the first of these systems. They were using three separate microprocessor circuits in a redundant system, with a voting circuit that required two or more of them to agree on what to do next. (If you only have two microprocessors, you have to 'safely shut down if their outputs disagree, with three you can keep going unless all three outputs disagree)

To help avoid problems with EMI and software bugs, they did the following:

- Each of the three microprocessors were designed and made by different companies, and shared no common design background – were "architecturally diverse" (e.g. had not been developed from any common "ancestor" microprocessor).

  The idea being that any hardware errors would arise at different time, under different stimuli, and that their response to EMI and similar "common cause" problems (e.g. over-temperature) would be different.

- Each microprocessor ran software that used a different programming language from each other, the programming languages being "architecturally diverse" – that is, they were not derived from a common ancestor language.

  The idea being that any bugs would arise at different time, under different stimuli, and that their response to EMI and similar "common cause" problems (e.g. over-temperature) would be different.

- The three teams that wrote the three sets of software had never worked for the same companies, or studied at the same universities. They worked in different buildings and had no contact with each other.

  The idea here is that certain programming habits (not necessarily bad ones) such as short-cuts or the use of undocumented features of the software language, would not then be replicated between the three software programmes, to help

avoid the possibility that their software might misbehave under certain common circumstances, at the same time.

As you can see, the idea is not to try to make each microprocessor circuit and its software reliable enough for safety (which is almost certainly impossible without using military software languages such as ADA, which can be mathematically proven) – it is to make sure that when any one microprocessor fails, the other two are still OK. Remember that the voting circuit that decides if it has a two out of three consensus is making these decisions thousands of times each second, maybe tens or hundreds of thousands of times each second.

About a decade later, I happened to meet the guy who gave that presentation at Savoy Place, and told him how impressed I had been by it. He looked downcast, rather than pleased to be congratulated, so I asked why. He told me that each of the three independent software teams had all been working to the same "Requirements Specification" – and that this had some bugs in it (in other words, it failed to describe exactly the correct requirements for every aspect of flight control – it had mistakes in it). So of course all three teams wrote their software programs to achieve the same (flawed) results and the aircraft had problems which required very costly redesign.

He said that in hindsight, they should have had three different teams writing three different versions of the requirements specification, working in different buildings and having no contact with each other, and never having worked for the same companies or studied at the same universities, etc., etc.

Writing 100% perfect requirement specifications for software is very difficult indeed, and very rarely achieved in practice [6].

Compare this approach with the one used in the auto industry, where all the functions that are called backup or fail-safe systems are *not* independent of the computer control and so have only a limited effect in increasing the reliability of the complex electronics.

Also consider the statements made by Toyota that they use dual-redundant microprocessors in their engine control units. But unless those processors are "architecturally diverse" and run different software with is itself "architecturally diverse" what were designed based on requirements specifications written by different teams – then the redundancy does not provide any additional protection against software errors (bugs) or EMI.

6 EMC testing cannot *prove* EMI immunity for safety-critical systems

EMI has long been recognized as a cause of unreliability in electronic equipment, especially by the military and aero-space industries, and as a result EM immunity test methods and regimes have been developed.

These tests have generally been successful in reducing the failure rate due to EMI. Given the great difficulties in deter-mining whether a given undesirable incident was caused by EMI, the lack of incidents officially assessed as being caused by EMI has led some people to feel that current EMI testing regimes must therefore be sufficient for any application. Indeed, it is commonplace to read words such as "….*passes all contractual and regulatory EMC tests and is therefore totally immune to all EMI."*

However, as Ron Brewer says in [8]:

> "*…there is no way by testing to duplicate all the possible combinations of frequencies, amplitudes, modulation waveforms, spatial distributions, and relative timing of the many*

> *simultaneous interfering signals that an operating system may encounter. As a result, it's going to fail."*

[9] says:

> "*Although electronic components must pass a set of EMC tests to (help) ensure safe operations, the evolution of EMC over time is not characterized and cannot be accurately forecast."*

Expanding on the "10,000 vehicles tested continuously for six months" example above, since EM phenomena are tested one at a time, if we were testing for auto electronics resistance to various electromagnetic phenomena, and if we assume five different kinds of tests are needed, we would need to have 50,000 EMC test laboratories all testing vehicles at the same time continuously for six months.

In fact, vehicle manufacturers will test just a few vehicles in their EMC test labs for a week or so each, to "prove" EMC. When any EMC tester says, "*Our products pass all our very stringent EMC tests in our 32 million dollar test chamber. Therefore they are totally immune to all forms of EMI*," all this proves is that the tester doesn't understand how very limited his range of test stimuli is compared with the real world. Also, he or she doesn't understand anything at all about design verification, especially where safety issues are concerned. Nothing can ever be made totally immune to EMI. It's all a question of cost versus risk.

Here's a relevant quotation from a Ford internal document. It concerns the effectiveness of testing (note that DV stands for Design Verification, and EED for Electronic Engineering Division): DV TASK FORCE REPORT 8/30/85:

> "There exists a prevalent misconception in EED that DV is a set of tests used to endorse a final design. This is a degradation of the original intent of the DV process. *A small sample of vehicles or components is incapable of assuring that robust designs will be released.*" (my italics).

Notice here they are talking about design verification in general, not about design verification for safety-critical vehicle systems such as throttle controls. (Mind you, in a document dated October 31, 1989, Ford listed cruise controls under "Convenience and Entertainment," not under "Affects Vehicle Operation"!)

As I was writing this article, I once again saw in the daily news an automobile manufacturer stating that "*None of our EMC testing has ever caused a sudden acceleration, therefore EMI cannot be a cause of sudden acceleration*." And so, once again, just about all the auto manufacturers have used this feeble attempt as an excuse over the last 30 years, Toyota being the latest to trot it out.

Although they really mean nothing at all, such statements sound persuasive to people who aren't specialists in electronics, EMI or statistics. The very simple analyses in this section and the previous one show that one should not expect any practical EMC testing to cause a sudden acceleration. The statistics mitigate finding any such thing.

I am not saying that it is impossible to do EMC tests that could replicate sudden acceleration in the laboratory - just that the application of the normal testing regimes to vehicles chosen at random should not be expected to find anything.

The problem with all electronics is that it is time-dependent, and (especially a microprocessor running software) can have many millions of different states, maybe hundreds or thousands of millions, each one lasting for as little as a few nanoseconds (thousand-millionths of a second),

with each state having a different susceptibility to upsets such as EMI, which is also time-dependent.

Testing computer (microprocessor) based systems for susceptibility to EMI is like trying to find a needle in a haystack (the few very susceptible circuit states out of the hundreds of millions) by sight alone in the pitch dark, with the only illumination coming from a camera's flashgun (the EMI test).

Leaving aside the statistical argument above for a moment, a few simple examples suffice to shut up the "EMC testing is sufficient" brigade. For example, the fact that in safety engineering, products are always tested with reasonably foreseeable lifetime faults simulated means that the product stays safe despite the occurrence of a likely fault. The product might not work with the fault in place, but at least it is safe.

In a modern auto electronics module there are many foreseeable (even likely) faults that will remove the module's protection against one or more of the normal electromagnetic phenomena it is exposed to. But EMC testing is only ever done on new modules or new vehicles with fault-free construction.

Indeed, if any manufacturing faults are found in modules or vehicles during EMC testing, they are fixed and the tests redone. However, they don't fix their manufacturing process to stop it from producing overly susceptible vehicles from time to time!

Here's a real-life story from Michel Mardiguian (m.mardiguian@orange.fr), a French EMC expert who specializes in tracking down EMI problems for automakers. On a cold day in 2005, an auto maker's employee started a preproduction model in his driveway and began wiping the dashboard with a cloth, when the air bag blasted into his face. The manufacturer suspected electronics and called in Mardiguian.

He worked with their engineers, hitting the air bag sensor with multiple types of EMI, including using an electrostatic discharge (ESD) simulator (a Taser-like device) to create static electricity and turning the heater on just like the driver did. Four days of extensive testing passed, during which the ESD testing reached 27,000 Volts (normal vehicle ESD testing stops at 15,000 V), but the air bag problem couldn't be reproduced.

Finally, someone mentioned that, during assembly, sometimes a twisted-pair cable from the airbag sensor would get trapped, pinching one of the wires and shorting it to the body of the vehicle. When the ESD tests were repeated on vehicles with the trapped wires, and the heater turned on, the airbag could be made to operate when it shouldn't. They had finally managed to recreate the original problem, but it required three separate things to happen at the same time.

But when you have millions of vehicles on the roads, unlikely combinations of events happen very often.

In addition to not testing with simulated faults, as is done with all proper safety testing, there are at least seven more reasons why current vehicle EMC testing is inadequate and/or insufficient where safety is concerned:

- The tests do not simulate real-life electromagnetic environments (e.g. the use of anechoic chambers for radiated RF immunity testing from a few angles (to save time) when in real-life the environment is reverberant, not anechoic, so radiated waves arrive from any angles, and from many angles at once.)

- The tests do not simulate real-life EMI threats (e.g. a wide range of modulation types and frequencies, a wide range of surge and transient waveforms, and the simultaneous

existence of two or more EMI threats, for instance ignition “spikes” plus ESD, plus radiated RF at two or more frequencies at once).

> If anyone tries to tell you that the type of modulation and/or its frequency has no effect, they are just revealing their ignorance of how electronic circuits respond to EMI. The latest version of the avionics EMC test standard RTCA DO160F and of the military EMC test standard MIL-STD-461F, recommend testing with amplitude modulation at the frequencies to which the equipment under test is most susceptible. Some senior members of the teams producing these standards think these requirements should be mandatory.

- EMI ‘risk assessment’ is not done. EMI is not treated as a safety-related issue.

- The effects of the physical/climatic environment, that can affect resistance to EMI, are not considered (mechanical bending forces, shock, vibration, humidity, condensation, freezing, high temperatures, thermal cycling, mould growth, etc.)

- Only a small sample is tested, so errors in assembly that reduce resistance to EMI can remain in vehicles delivered to customers.

- Emergent behavior. A vehicle is a single very complex electronic system, made from a variety of modules and subsystems, the subsystems themselves in turn made of various modules. But the EMI behavior of the subsystems and the overall vehicle system cannot be predicted from the EMI behavior of the modules when tested on their own. This is known as “emergence” – a well-known phenomenon in systems integration, but mostly ignored by EMC engineers working for manufacturers.

- Shortcomings in the ‘performance criteria’. The functional performance requirements used when testing modules for their resistance to EMI, can be inappropriate for the system as a whole.

For more on this, see Section 0.7 in the IET’s 2008 Guide [1].

When automakers rely on testing as their only way of verifying the EMC of safety-related systems, what they are really doing is using their customers to do the final EMC design verification of their vehicles. Once you have a few hundred thousand vehicles on the road, in all weathers and in all conditions, you really start to find out how robust your design was!

"Electromagnetic interference leaves no trace," Mardiguian says "It goes away just as it came." He goes on to say: "An automaker who declares bluntly that uncontrolled acceleration cannot be caused by EMI because they have fully tested their vehicle is a liar, or naive".

7 Auto electronics do not employ safety principles that have been commonplace, even mandatory, in many other industries for decades

7.1 “Fail safes” or “Backup Systems” must be independent systems

Since 2000, IEC 61508 [2] has codified the international best practices to be used when safety engineering the hardware and software of complex electronic systems - basically, anything that uses a microprocessor. The UK’s Health and Safety Executive use it as their guidance when assessing the safety of industrial control systems and the like.

IEC 61508 [2] makes the perfectly reasonable assumption that complex electronic systems cannot be relied upon to be safe enough for most purposes. Instead, independent “safety

systems", "backup systems" or "fail-safes" are required to be added to reduce the risks to acceptable levels. Sometimes two or more independent systems are necessary to achieve tolerable levels of safety.
[4] says:

> "The architecture of the safety-critical-system should avoid major hazards wherever possible (for example, by backup systems of low complexity or mechanical interlocks) so that the degree of dependence on software-based systems is kept as low as reasonably practicable and single points of failure are eliminated."

This means that you shouldn't rely on the computer for safety, but instead should fit at least one independent fail-safe or backup system that uses simple technology and so can be engineered to be very reliable indeed.

The use of independent low-technology backup systems and fail-safes has been standard practice in computer-controlled machinery, in Europe and the USA, for many decades.

But the automobile industry continues to ignore standard safety engineering principles such as this, even though a modern vehicle is actually a computer-controlled machine. I understand that they do this to save a couple of dollars on the cost of each vehicle.

Safety systems can use any appropriate technology, but because the same technologies tend to react to EMI in the same ways, they should use different technologies from the computer system they are protecting us against, and (where there is more than one safety system) they should use different technologies from each other.

The design of the safety systems can be assessed, verified and validated using a wide variety of techniques (not simply testing) to achieve the level of safety risk considered acceptable by the user.

When safety systems use simple, "low-tech" designs, such as certain mechanical technologies, it can be possible to prove they are reliable enough using very simple and quick assessment, verification and validation methods.

For example, pure mechanical, hydraulic and pneumatic technologies have no susceptibility to EMI (short of direct lightning strike that melts their parts!), and – since they do not exhibit time-dependent behavior like electronic circuits and software – one simple set of tests (e.g. a strength test that applies a level beyond the worst possible overload, plus a wear-out test that simulates more than a lifetime's heavy use) may be sufficient.

I am not aware of any vehicle manufacturer who has a real backup or fail-safe system implemented on the throttle control. Though many have devices that they *call* "fail-safes," in fact they are not, because they aren't independent systems.

Generally (like the so-called "smart brake" systems with which some vehicles are fitted that close the throttle when the brake is pressed regardless of the position of the gas pedal) these fail-safes are nothing more than a few extra lines of software running on the engine/throttle control computer - the very electronics that needs an independent backup or fail-safe system in case it malfunctions!

7.2 Making the driver the backup for vehicle control failure is bad practice

In almost every field, the operator is not generally made responsible for operating (or being) a safety system, except in special circumstances where the operator has been trained to deal with the specific situation, *and* there is sufficient time for him to respond correctly.

However, another favorite excuse of the auto makers is to pretend that a driver should always be able to respond correctly, in a split second, to a failure mode they've never dealt with before and have not been trained to deal with, for example, a high-revving engine that can't be stopped without turning off the ignition.

Making drivers the back-up systems for poorly designed safety-critical systems they have not been trained in, is just plain bad safety engineering practice.

When you realize that the startling effect of a completely unexpected and unique vehicle failure mode can last for two to three seconds, and think of how much damage you could do on a busy road with a vehicle running amok for that length of time, you can see how stupid it is to even imagine that it is acceptable to expect the driver to regain control quickly enough.

All this is before we consider the ineffectiveness of standard braking systems when faced with a wide-open throttle, an engine that has reached 4000 rpm or more, and rear-wheel (or 4-wheel) drive through an automatic transmission, as mentioned earlier.

Front wheel drive vehicles are easier to stop, because the brakes on the front wheels are so much more powerful than those on the rear. But that does not mean a front-wheel-drive vehicle with its engine racing at full-throttle is going to be easy to stop! Also, brake pads are not designed for stopping a vehicle under such conditions, so will overheat and fade, reducing braking effectiveness.

In the USA people seem to believe that pumping the brakes (repeatedly releasing and pressing the brake pedal) is what you do if braking effectiveness seems too little. As explained earlier, with a high-revving engine the vacuum boost for the brake servo is not replenished, so pumping the brakes has the exactly opposite effect of what is intended - brake boost is reduced and braking efficiency is lost. Of course, no vehicle's Owners Manual includes such a warning. Yet still the automakers trot out their line about drivers being in control of their vehicles.

8 Standards

The International state of the art for how to achieve functional safety is IEC 61508 [2]. It assumes that complex electronics cannot be made safe enough, and that they will need at least one additional truly independent fail-safe that uses a different technology (so doesn't suffer from the "common cause" problems typical of EMI) to achieve acceptable levels of safety risk.

IEC 61508 was first published in 2000 and its second edition is imminent. The auto industry has only recently produced a first draft of its version - ISO 26262 [3], which is several years from publication and then will need several more years before it is adopted as normal practice.

9 Lead-free soldering

In recent years, various countries and trade blocs (including the European Union) have mostly banned the use of lead on electrical solder, on the basis that lead going into landfill when electrical and electronic products are disposed of is bad for the environment, and hence for people. But many accuse them of being short sighted - lead has been added to solder in quite large amounts for many decades because it made the other main constituent, tin, behave much better, considerably improving reliability.

But when lead is been removed from solder, which is then mainly tin (with a little silver and copper added), all sorts of new possibilities arise for short-circuits and open-circuits, and intermittent shorts and opens, mainly on printed circuit boards (PCBs) and mainly associated with small-footprint integrated circuits (ICs), especially ball-grid arrays (BGA's).

It's really just another cause of intermittent or fixed short-or-open circuits in electronic PCBs and modules - but one that would not have been any problem until a few years ago, and so could have caught Toyota by surprise if their suppliers used lead-free soldering.

John R Barnes has created a monumentally huge library of references to the problems of lead-free soldering, especially tin whiskering, www.dbicorporation.com/rohsbib.htm. Prepare to be totally overwhelmed! Removing lead from solder has the following effects:

9.1 Tin whiskers

These will grow out of soldered joints and can contact other conductors, causing short-circuits between PCB copper traces and the pins of connectors. They are often no longer than 0.5mm (about 1/50th of an inch) but can grow to 1mm (about 1/24th of an inch) or longer, especially in damp conditions. Even at 1/50th of an inch they can short between the pins on a modern integrated circuit (IC). And the process of removing the PCB for inspection can brush them off, so you never find them. And if you didn't accidentally brush them off, they are so thin they are very hard to see - you need a powerful microscope. They are as fine as the finest spider-web threads, yet can carry sufficient current to short out the electronics. You won't see them unless you are looking for them.

Being so thin, they can wave around in the breeze and/or due to shocks, vibration and acceleration, and also be broken off by these events and rattle around inside a unit, causing intermittent short-circuits. When a unit is opened up, loose tin whiskers can fall out or be blown away by a breath, and so not be noticed.

The iNEMI organization has published guidelines [X] on how to ensure that tin whiskers don't grow too long, but I don't know to what extent these are followed by suppliers of electronics to the car industry in general, or Toyota in particular.

Electronic engineers will note the questionable quality of the terminal's solder joint that potentially will make it very unreliable, This poor soldering was typical of about 50% of the joints on the PCB, suggesting that the manufacturing quality control of the company that supplied the printed circuit board assembly and the pedal assembly were manifestly deficient.

9.2 Dry or brittle solder joints

Solder joints made using lead-free solder are less resilient, more brittle, more prone to cracking, especially in areas with large temperature excursions and vibration (e.g. motor vehicles), and especially under large devices such as BGA's - resulting in more open-circuits on PCBs.

These cracks may be invisible without X-Ray inspection, and will often be intermittent. For example: when the PCB is mounted in its box and mounted on the vehicle, it is bent slightly and that opens the connection or makes it subject to vibration and/or temperature changes (due to differential thermal expansions). But when the PCB is taken out for inspection, it tests just fine.

Cracked solder joints causing intermittent or open-circuit connections have always been a problem, but are made worse by lead-free soldering.

A particular problem occurs when an EMI shunt-filter component, such as a capacitor, experiences a "dry joint" or a cracked and intermittent solder joint. When the joint is open-circuit, EMI is allowed into the electronic circuit, where it can cause errors or misoperation. But when the circuit is tested for functionality, it tests just fine, even if the filter's joint is still open-circuit. Of course, after the ignition has been turned off, no trace of the error or misoperation remains.

Diagnostic testers, as used by Auto Dealers, do not test for such things as broken solder joints in EMI filters. Functional testers as used by the automaker or their suppliers also don't test for this sort of thing. The two sensors boards from the CTS gas pedals that I have seen, were more badly soldered than anything I have ever seen on any product ever before – so I would not be at all surprised if they had one or more dry (open-circuit) joints. And since almost all of the components were capacitors for EMI shunt-filtering, it would not be surprising to find that one or more filters on those pedals were actually disconnected, leaving the gas pedal sensors (complex ICs in their own right) vulnerable to EMI.

9.3 Tin Pest

Lead-free tin tends to revert to a different crystalline structure, which means it becomes just grey dust and falls off or is blown away by a breeze. Obviously, this creates an open-circuit solder joint, one that is easily spotted if it occurs.

9.4 Higher soldering temperatures can weaken components

Lead-free soldering has to use higher temperatures, and this increases the stresses on the components that are mounted on the board during the soldering process.

Another issue is that the range of temperatures for lead-free soldering is not only higher than for traditional solder, it is also narrower. Some PCB-assemblers soldering equipment may not be able to maintain the temperature within the required bands at all times, causing an increased number of bad joints and/or heat-damaged components. As a result, the actual components (especially ICs) may test sufficiently when newly assembled, but fail or behave incorrectly when in use, due to internal changes that require an electron microscope to be seen.

10 Software

I am not competent to write about software, so I won't say more than that some software programs can be unstable when faced with combinations of inputs that their designers did not anticipate or deal with correctly. EMI is one way of 'confusing' software so that it behaves in ways never dreamed of by its designers.

IEC 61508-3 is all about how to design and verify software for safety-critical systems, but, as far as I am aware, no auto manufacturer uses it. The draft ISO 26262 doesn't include the same guidance, so they probably never will.

11 References

[1] The IET's 2008 Guide on EMC for Functional Safety. Free download from www.theiet.org/factfiles/emc/index.cfm, or purchase as a colour-printed book from www.emcacademy.org/books.asp

[2] IEC 61508:2000, "Functional safety of electrical/electronic/programmable electronic safety-related systems", from www.iec.ch. It has 7 parts. Soon to be published as its 2nd Edition.

[3] ISO 26262 (draft, 2009), "Road vehicles - Functional safety", from www.iso.org. In 10 parts.

[4] IET Position Statement on Computer Based Safety-Critical Systems, www.theiet.org/factfiles/it/computer-based-scs.cfm?type=pdf

[5] "This Car Runs on Code", Robert N. Charette, IEEE Spectrum, February 2009, http://spectrum.ieee.org/green-tech/advanced-cars/this-car-runs-on-code
"It takes dozens of microprocessors running 100 million lines of code to get a premium car out of the driveway, and this software is only going to get more complex"

[6] "Why Software Fails", Robert N. Charette, IEEE Spectrum, September 2005, http://spectrum.ieee.org/computing/software/why-software-fails
"We waste billions of dollars each year on entirely preventable mistakes."
Although this article tends to focus on large computer projects, it applies equally well to any complex software design project, such as the software controlling a modern vehicle (see [5])

[7] Prof. Nancy Leveson, "A New Accident Model for Engineering Safer Systems", Safety Science, Vol. 42, No. 4, April 2004, pp. 237-270, http://sunnyday.mit.edu/accidents/safetyscience-single.pdf

[8] Ron Brewer, "EMC Failures Happen", Evaluation Engineering magazine, December 2007, www.evaluationengineering.com/ features/2007_december/1207_emc_test.aspx

[9] Alexandre Boyer et al, "Characterization of the Evolution of IC Emissions After Accelerated Aging", IEEE Trans. EMC, Vol. 51, No. 4, November 2009, pages 892-900

[10] iNEMI Recommendations on Lead-Free Finishes for Components Used in High-Reliability Products, Version 4 (12-1-06)
http://thor.inemi.org/webdownload/projects/ese/tin_whiskers/Pb-Free_Finishes_v4.pdf
iNEMI High-Reliability Task Force Position Statement on RoHS5 & RoHS6 Subassembly Modules,
http://thor.inemi.org/webdownload/projects/ese/High-Reliability_RoHS/High_Rel_position_061206.pdf
Also see:
JESD201, "Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Tin Alloy Surface Finishes" http://www.jedec.org/DOWNLOAD/search/JESD201.pdf
JP002, "Current Tin Whiskers Theory and Mitigation Practices Guideline"
http://www.jedec.org/DOWNLOAD/search/JP002.pdf
iNEMI's "Recommendations on Lead-Free Finishes for Components Used in High-Reliability Products" (v3, updated May 2005)
(http://thor.inemi.org/webdownload/projects/ese/tin_whiskers/User_Group_mitigation_May05.pdf)
iNEMI Tin Whisker Acceptance Test Requirements (iNEMI Tin Whisker User Group, July 28, 2004)
(http://thor.inemi.org/webdownload/projects/ese/tin_whiskers/Tin_Whisker_Accept_paper.pdf)

[11] NHTSA Final Report, April 30, 2008 "2007 Lexus ES-350 Unintended Acceleration", enclosing "VRTC Memorandum Report EA07-010, VRTC-DCD-7113, 2007 Lexus ES-350 Unintended Acceleration".
I can provide a copy if required, and/or a copy of a critique of it by my colleague, Dr Antony Anderson, www.antony-anderson.com

[12] Melexis MLX 90277 Data Sheet, download from:
www.melexis.com/Sensor_ICs_Hall_effect/Linear_Hall_ICs/MLX90277_381.aspx