Another EMC resource
from EMC Standards

The Poor Quality of Functional Safety Engineering in the Automobile Industry

Helping you solve your EMC problems

9 Bracken View, Brocton, Stafford ST17 0TF T:+44 (0) 1785 660247 E:info@emcstandards.co.uk

As published in "In Compliance Magazine"
http://www.incompliancemag.com/index.php?option=com_content&view=article&id=491:the-poor-quality-of-functional-safety-engineering-in-the-automobile-industry&catid=25:standards&Itemid=129

November 2010

Written by Dr. Antony Anderson, Dr. Brian Kirk, and EurIng Keith Armstrong

An Open Letter to the NAS team working on the project: Electronic Vehicle Controls and Unintended Acceleration (TRB-SASP-10-03)

The professional opinions of Dr. Antony Anderson BSc(Hons), PhD, CEng, FIEE/IET MIEEE, Dr. Brian Kirk BSc(Hons), PhD, CEng, MBCS, MACM, and EurIng Keith Armstrong BSc(Hons), CEng, FIET, SMIEEE, ACGI

Summary

The three decades-old problem of sudden unintended acceleration – that only occurs in cars fitted with automatic gearboxes and electronic systems directly controlling their throttles – has led us to write this letter. It explains why we believe that Government Regulators must now mandate the use of functional safety techniques in the automotive industry, based on the approach used in all other safety-related industries, i.e. independent safety assessment to peer reviewed public functional safety standards.

Unlike other industries that use electronics to control safety-critical functions, the automobile industry does not employ peer-reviewed public functional safety standards or independent safety assessors to verify conformance to such standards. Presently we are expected to simply trust whatever automakers assert about the safety of their products!

The auto industry is probably the only industry in the world allowed by Government Regulators (such as NHTSA in the USA) to behave in this way regarding risk to the Public. Certainly, the rail, aviation and medical device industries are not allowed such freedom – despite the fact that, every day, many more people are exposed to lethal hazards from automobiles.

Rather than accept responsibility automakers are content to blame drivers, even when accidents could have been caused by malfunctions of electronics based driver assistance systems. Unfortunately, for well over a decade the Regulators have demonstrably failed to intervene in this area with any effect.

If the problem of the poor quality of functional safety in the design and manufacture of automotive systems is not promptly addressed then we expect the current and next generation of vehicle electronic systems to result in considerably increased carnage on the roads in future.

Background

In the early evening of 28th August 2009, an off-duty California Highway Patrolman was driving a hired 2009 Lexus ES 350 saloon (sedan) when it suddenly accelerated to about 120 mph shortly before reaching a T junction. The runaway vehicle hit a Ford Explorer, crashed through a fence, flew into the air, turned over twice and fell into the flood plain of the San Diego River, where it exploded in a ball of fire.

Mark Saylor a skilled police driver with 19 years experience and inspector of heavy vehicles, his wife, 13 year old daughter and brother-in-law were killed instantly. The last 48 seconds before the crash were recorded in a dramatic 911 call which captured the horror of the event.[1]

As one newspaper put it: “Rarely, if ever, has one family’s fatal crash had such an impact, forcing the world’s largest automaker to admit thousands of sudden-acceleration complaints, recall more than 8 million vehicles worldwide and answer growing questions from Congress and consumers about its safety record.”[2]

However, in spite of the recalls to check floor mats and fixings or to insert shims to prevent the possibility of sticky accelerator pedals, sudden unintended acceleration incidents are still occurring in Toyota vehicles that allegedly have

been fixed. The fact that a skilled police driver like Mark Saylor would have been perfectly capable of dealing with such problems adds to the strong suggestion that the causes of sudden unintended acceleration have not been sufficiently addressed and probably lie elsewhere.

Toyota categorically denies the possibility of malfunctioning electronic throttle controls. This denial makes it appear, by default, that drivers are to blame and the cause of their own misfortunes: apparently failing to be in control of their vehicles at all times, as the law requires. It is not clear on what factual basis Toyota make their assertions. Thus, in extremis, because the vehicle electronic systems are given the benefit of the doubt, the drivers of suddenly accelerating vehicles are punished for allegedly reckless driving. However we assert that in many cases it should be the automobile manufacturers who should be punished for reckless inattention to the requirements of functional safety.

Absence of Proof is Not Proof of Absence of an Intermittent Electronic Malfunction

In mechanical systems, such as the throttle controls in vehicles from before the 1980s, evidence of malfunction is usually present after such an event. However, electronic systems are different. An intermittent electronic error or malfunction may only appear as a result of a rare combination of many factors and may not reappear for years – if ever. Some errors and faults will not trigger fault codes that are recorded in an Electronic Data Recorder (EDR), as Dr David Gilbert demonstrated to Congress in February 2010,[3] and few can be reproduced to order later. Professor Todd Hubing has reported more extensive results along similar lines in July 2010.[4]

This is a situation in which absence of proof is not proof of absence. It is our opinion that “no electronic fault found” after a sudden unintended acceleration incident should never be taken to mean proof of the absence of an electronic fault causing that incident. Particularly when the recorded data concerning the incident can only be accessed by the manufacturer.

Yet again and again in post-incident vehicle examinations the fallacious argument that absence of proof is proof of absence is used to exonerate the vehicle manufacturer and transfer blame to the driver. We believe it is high time that the automobile industry acknowledged the reality of intermittent electronic errors and malfunctions (which has always been a plain and simple fact of life for all other manufacturers of electronics in all other applications) and stopped claiming their non-existence.

Much as they would like us to believe that it is so, the auto industry has no magical “pixie dust” with which to treat its electronics – it is stuck with the same laws of physics as all other industries.

Complexity of Vehicle Electronic Systems and the Impossibility of Testing for All Possible Failure Modes

Such is the complexity of the electronic systems in modern vehicles that it is totally impossible to completely test to eliminate all possible dangerous failure modes, either of hardware or software, before going into production. See Annex A for the explanations.

The false and unjustified assumption of the supposed near-perfection of safety critical electronics is likely to prevent the inclusion at the design stage of safety measures designed to anticipate and mitigate any possible effects of an electronic error or malfunction. In our opinion, the manufacturer’s omission of an independent fail-safe against a stuck-open throttle, i.e. one that would reduce the engine power in an emergency, is the most likely reason that prevented Mark Saylor from bringing the runaway Lexus safely to a halt.[5]

Investigative Studies into Sudden Acceleration by NASA and NAS

As a direct result of the questioning from Congress, NHTSA have recently commissioned two investigative studies, one by NASA[6] into sudden unintended acceleration in Toyota vehicles and the second by the National Academy of

Sciences (NAS)[7] into the possible electronic causes of sudden unintended acceleration in general. It is to this second investigative committee that this memorandum is addressed and in relation to the matter of functional safety.

Independent Fail-Safes – How the Automobile Industry Differs from the Rest of Industry

In our opinion, the absence of an independent fail-safe to protect against sudden unintended acceleration is a clear indicator that the automobile industry does not pay sufficient attention to the functional safety of vehicle electronic control systems. In other words the quality of the functional safety incorporated into electronic acceleration and braking control and management is poor at best, i.e. not fit for purpose nor capable of verifiable safety.

Generalizing from the Saylor case and other examples, it seems to us that the necessary attention to functional safety in regard to the design of electronic control systems in automobiles is manifestly lacking. In all other industries an independent fail-safe would usually be incorporated.

Even where independent fail-safes are used, “means of last resort” protection is usually provided – witness the emergency stop buttons on escalators and factory machinery. Even the domestic water supply has a stopcock and, even though household electrical circuits are very well protected by fuses and circuit-breakers, they still always have a manual ON/OFF switch.

But ignition keys in automobiles are increasingly being replaced, as in the Lexus ES-350, with buttons that require pushing for several seconds to switch an engine off – seconds that are almost impossible to find when one needs both hands on the wheel to press down hard on the brake whilst simultaneously steering to avoid hazards caused by high speed or extended stopping distance.

However in the automobile industry it appears to be thought entirely acceptable that – in the event of a sudden unintended acceleration – the driver should, by hard braking action, be able to overcome the engine with the brakes and bring the vehicle safely to a halt.[8] The driver is unwittingly made the “fail-safe” for the electronic throttle. Worse still the effectiveness of this fail-safe depends on the reaction time, physical fitness and stamina of the driver!

Functional Safety

The term “functional safety” may not be familiar, but it simply concerns the safety risks that could result if a product or system does not perform its activities (its functions) correctly and safely.[9]

Automobiles have a number of interacting safety-critical control functions – engine speed control, gearbox, braking, steering and stability, for example – that must work together. These functions have to be specified, designed and manufactured to be adequately operationally safe both individually and together. Therefore these various control systems must be analyzed individually and together at the design stage from the point of view of their capability to cause functional safety risks.

By the early 1990s the old approach of always fitting a low technology back-up or fail-safe to any safety-related electronics had become inadequate. It had also become well established that it was impossible to do enough testing to prove that electronic devices and systems (and their software programs) were acceptably safe for safety critical applications (see Annex A for details).

Further, there were also many new safety improvements that could be made, provided that the electronics and its software programs could be made much more reliable than normal.

For these reasons, a great deal of work in academia, industry and standards committees was carried out during that decade on how best to make safety-related software and electronic hardware reliable enough for the achievement of acceptable functional safety risks. The resulting standard on how to achieve “functional safety” of electronic (especially computerized) devices and systems was published in 2000 as IEC 61508.[10,11]

Since 2000, many industries (including machinery, rail and aviation) have carried out international peer-reviewed processes lasting several years to interpret the basic functional safety standard IEC 61508 in terms more relevant to their own applications, thereby creating several industry-specific standards on functional safety, for example, EN 50128.[12]

The auto industry has recently started to develop a public standard on Functional Safety, based upon IEC 61508, called ISO 26262.[13] However, ISO 26262 was only at its first draft in 2009, when the machinery, rail and aviation industries had not only already created their standards, but their independent safety assessors had been using them for many years.

The first draft of ISO 26262 is deficient in many ways.[14] Indeed, it is arguable that ISO 26262 is unnecessary, because the existing IEC 61508 standard – combined with a new standard defining the safety considerations specific to the auto domain – would provide a quicker solution which could make use of the widespread safety auditing services already available from other industries.

It remains to be seen whether ISO 26262 will ever become a published standard – let alone an effective one in terms of safety outcomes for consumers. But even if/when it is published as a public standard, the auto industry appears to lack the necessary disciplines of holistic system design and of independent safety assessment that would ever make functional safety a reality within the industry.[15]

Significant cultural and structural changes are required within the industry and its regulatory institutions to be able to develop a functional safety culture appropriate for the modern and future automobile.

Independent Safety Assessment Against Peer-Reviewed Public Safety Standards

Other industries that use electronics to control safety-critical functions – such as nuclear, chemical, machinery, air and rail transport – rely on independent assessment of their product's functional safety against public peer-reviewed safety standards.[16]

If an independent safety assessor (ISA) doesn't agree that the evidence and arguments presented about the specification, design and realization of a product demonstrate that it has acceptable levels of functional safety risks, then design changes have to be made to assure verifiable safety and thus demonstrate conformance with the safety standards to the ISA before the product can be supplied to customers. ISAs employ a variety of verification and validation methods, including both analysis and testing, but (as noted earlier) testing alone cannot be relied upon because it is incapable of providing enough data to show that a product or system will be safe enough over its anticipated operational lifetime (see Annex A).

The auto industry is the exception to general industrial practice because such functional safety engineering as it does is conducted behind closed doors, using internal specifications that have not been publicly peer-reviewed, and the resulting vehicles are sold to customers without any independent approval of their functional safety. The resulting lack of transparency of the manufacturers evaluating recorded data from vehicles calls in to question its value as evidence. The possibility of undetected tampering with the data by the manufacturers or others also needs to be addressed. These issues do not arise in other industries because data recorders and their contents are evaluated by independent third party assessors.

With the electronic complexities of some modern automobiles – the number of lines of software code (circa 100 million) are now far greater than in an F35 Joint Strike Aircraft (circa 5.7 million)[17] – there ought to be at least as much attention paid to functional safety at the design stage of a new automobile as there is in for a new aircraft.

Also, in other industries, e.g. aviation and avionics, there are schemes whereby safety problems and concerns can be reported to the industry while guaranteeing anonymity to protect the contributor. The automobile industry has no such scheme, and, unlike other industries, not much is publicly known about how automakers control functional safety risks

because they will not divulge such information for “reasons of commercial confidentiality”.

Any lessons that automakers learn from complaints of vehicle malfunction are kept under lock and key, as are details of any “updating” of software that may be carried out when a vehicle goes in for servicing. Changes in software may in principle completely alter the behavior of the vehicle, for better or for worse, yet the automobile manufacturers keep that information secret.

It is normal in other industries for safety understanding and knowledge to be shared for the good of all, but in the auto industry, vested interests seem to take precedence. In effect, the automobile industry – unlike any other – is allowed to be the judge and jury of the need to ensure the functional safety of electronic control systems.

In all other safety related industries “taking a manufacturers word” that their products are safe enough, is regarded as utterly unacceptable! Yet the auto industry is permitted to operate on this principle!

In other industries, failure investigations – open to public scrutiny – recognize uncomfortable facts, endeavor to establish the truth and seek to determine the lessons that should be learnt from the failures. In this way a sound basis for an acceptable level of functional safety risk is established and is continuously improved. Not so in the automobile industry where there is a strong culture of denial of the existence of problems relating to functional safety.

When a threshold level of customer complaints is reached, the National Highway Transportation Safety Agency (NHTSA) starts to get involved. All too often the resulting investigation fails to carry out a proper epidemiological analysis of the complaints and gives scant consideration of the possibility of an electronic error or malfunction.

Both NHTSA and automaker’s lawyers initial reaction is to presume that drivers are to blame for accidents that could well be caused by errors or malfunctions in electronics or software, possibly instigated or exacerbated by EMC. This is most certainly not the approach taken by every other safety-related industry.

Self-regulation, as demonstrated by Toyota and other automakers in connection with sudden unintended acceleration incidents, evidently does not work.

It is our opinion that such are the potential risks implicit in the growing reliance on safety critical electronic control systems in vehicles that the automobile industry needs to become subject to the same disciplines regarding functional safety as other industries. Otherwise there will be increasing numbers of accidents caused by malfunctioning control systems – to cite a recent example, uncontrolled behavior of electronically assisted steering.[18]

We believe that the well established state of the art regarding functional safety in other industries – peer reviewed public functional safety standards based on IEC 61508, plus independent safety assessment – is what needs to be transferred to the auto industry now and is what the auto industry should be held accountable to in future by Government regulation.

EMI, EMC and Functional Safety Engineering

All electrical and electronic technologies – by their very nature – both cause and suffer from electromagnetic interference (EMI).[19]

Prior to the early 1960s electronics were associated primarily with radio communication, radar and television. Since it proved necessary to have EMC standards to ensure that radio and TV broadcasts could be reliably received without avoidable interference and likewise that multi-channel telephone and telegraph communication could take place with minimal interference between channels.

At that time, as far as the automobile was concerned, it was only necessary to ensure that the ignition system did not interfere with radio and television reception and with the vehicle’s radio reception.

The result is that the scientific and engineering communities associated with achieving electromagnetic compatibility (EMC) that have evolved since the 1940, grew up in a world in which there was little or no need to consider safety issues arising with safety-critical electronics because such electronics, especially in automobiles, did not then exist.

Those industries that started to apply electronic devices to the control of electrical machinery in the 1960s came from a very different background, in which electronics was assumed to be unreliable unless proved otherwise. So the new electronic technology had to be extensively proven against the old – and therefore manufacturers and users alike had to face the evident effects of EMI right from the beginning by adopting well-proven techniques for the minimization of its effects.

Nobody was going to allow the installation of any electronic control system in a power station, chemical plant, ship, aircraft or a train without full consideration being given to the potential consequences of electronic errors or malfunctions, what might happen as a result, and the provision of protective measures including independent fail-safes. From this need for a cautious approach to innovation came the wide scale emphasis on functional safety.

So we now have the situation where the scientific and engineering communities associated with functional safety, and those associated with EMI and EMC, don't share a common background, don't speak the same technical language, and often don't communicate with each other very well at all.

The functional safety experts who wrote IEC 61508 simply assumed that EMC testing was sufficient for safety – because they were told so by EMC experts who didn't (and still don't, in general) understand functional safety engineering. The result is that IEC 61508 and the other public standards derived from it have very few EMC requirements, they simply rely on EMC testing mostly intended to protect radio and TV channels from interference.

However, now that electronic systems are more widespread, and the voltages and currents they use are now much lower (and therefore equipment is much more susceptible to interference) and devices that emit electromagnetic radiation are much more common (e.g. Wi-Fi, Bluetooth, CB Radio, mobile phones, etc.) it is essential that EMC is included as an integral part of design for functional safety.

EMC testing suffers from exactly the same problem as software testing when it comes to functional safety – it is impossible in practice to prove by testing alone that an electronic device or system is acceptably safe (see Annex A).

Some credible reliance on correct design and integral functional safety mechanisms must be an essential part of the overall verification of the design and its manufactured product.

The first public "Technical Specification" (soon to become an approved standard) that attempted to deal with EMC for functional safety reasons was IEC TS 61000-1-2,[20] first published in 2000. Over the next few years, the EMC requirements in IEC 61000-1-2 will be incorporated into the functional safety standards as part of the process of continuing improvement.

Conclusions

It is our opinion that the automobile industry lacks the necessary framework at present within which to pay proper attention to functional safety of electronic control systems used in the vehicles they specify, design and manufacture. For example, there is no provision for the evaluation of vehicle electronics for sufficient functional safety by independent assessors. It would require significant cultural and structural changes to bring the automobile industry into line with functional safety practice in other industries. However, with the inexorable introduction of more and more interacting, electronic control systems such structural changes will become increasingly necessary.

If no action is taken to improve functional safety within the auto industry then there is no doubt that in future horrific accidents involving single and multiple vehicles will occur, due to their electronic systems being unsafe due to poor quality specification and design. When automated steering, convoy automation and other upcoming plans are implemented, the death toll from electronic system errors and malfunctions is certain to mount to the point where safety

regulation will have to be forced on the auto industry.

In the long term the automobile industry would benefit enormously from the introduction of independent functional safety assessments because it would provide a greatly increased level of confidence in the integrity of electronic control systems and circuit designs. Because electronic systems would have been subject to independent auditing, they would earn the right to be "trusted". At present, manufacturers' assurances regarding the functional safety of their products are pretty well meaningless. In effect manufacturers are currently asking motorists to put their trust in systems that are intrinsically untrustworthy and potentially dangerous.

Presently if a vehicle electronic system malfunctions, the driver is expected to take the blame for it. This appears to us to represent a complete abdication of responsibility by the automobile industry and its Regulators, in safety terms this amounts to negligence. By denying the possibility of electronic malfunctions and treating drivers as blameworthy by default, automobile manufacturers are denying themselves a vital source of feedback from customers in the field that should be leading to improved electronic functional safety to the benefit of all.

Annex A

Some quotations from world-class industry leaders supporting the fact that it is impossible to verify a modern electronics design (its hardware and/or software) by testing alone

From Alan M Turing, a mathematician and computing pioneer, in 1951

"It is of course important that some efforts are made to verify the correctness of the assertions that are made about a routine. There are essentially two types of method available, the theoretical and the experimental. In the extreme form of the theoretical method a watertight mathematical proof is provided form the assertion, In the extreme form of the experimental method the routine is tried out on the machine with a variety of initial conditions and is pronounced fit if the assertions hold in each case. Both methods have their weaknesses."

(Note: Instead of "routine" we would nowadays use "software," "program" or "firmware".)

From Edsger Dijkstra [21]

"Testing shows the presence, not the absence of bugs."

From Watts S. Humphrey, often called "The Father of Software Quality," Senior Member of Technical Staff, Software Engineering Institute (SEI), Carnegie Mellon University [22]

"Our programs are often used in unanticipated ways and it is impossible to test even fairly small programs in every way that they could possibly be used."

"With current practices, large software systems are riddled with defects, and many of these defects cannot be found even by the most extensive testing."

"Unfortunately, it is true that there is no way to prove that a software system is defect free."

From Jiantao Pan of Carnegie Mellon University [23]

"The difficulty in software testing stems from the complexity of software: we can not completely test a program with moderate complexity."

“Correctness testing and reliability testing are two major areas of testing.”

“Software testing is a trade-off between budget, time and quality.”

From Ross Anderson,Professor of Security Engineering at the Computer Laboratory, Cambridge University, UK [24]

“The critical problem with testing is to exercise the conditions under which the system will actually be used.”

“Many failures result from unforeseen input/environment conditions (e.g. Patriot).”

“Incentives matter hugely: commercial developers often look for friendly certifiers while military arrange hostile review (ditto manned spaceflight, nuclear).”

From Prof. Nancy Leveson, Professor of Aeronautics and Astronautics and Professor of Engineering Systems, Massachusetts Institute of Technology (MIT) [25]

“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.”

From the Goddard Space Flight Center, NASA [26]

“Software failures are rarely preceded by warnings while hardware failures are usually preceded by warnings”

“Software essentially requires infinite testing”

From The Institution of Engineering and Technology, the IET (formerly known as the Institution of Electrical Engineering, the IEE), London, UK [27]

“Computer systems lack continuous behavior 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. Systems that contain software will usually be far too complex for it to be practical to test them exhaustively”

“It is generally impractical to rely on test-based evidence in advance of putting a system into widespread service that the overall probability will be less than 10-5 per hour with 99% confidence, equivalent to a mean time between failures of approximately one year.”

From Professor Todd Hubing, Michelin Professor of Vehicle Electronic Systems Integration, Clemson University International Center for Automotive Research [28]

“Unintended automotive system behavior is a problem that will certainly get worse without a major change in automotive standards and design practices.”

From Michel Mardiguian, of Paris, France, renowned EMC expert who often works for the auto industry. [29]

“Electromagnetic interference leaves no trace, it goes away just as it came.” “An automaker who declares bluntly that uncontrolled acceleration cannot be caused by electromagnetic interference because they have fully tested their

vehicle is a liar, or naive."

From Ron Brewer, NARTE Certified EMC Engineer, IEEE EMC Society Distinguished Lecturer. Ron works on the EMC of the Space Shuttle and other space vehicles. [30]

"…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."

From Alexandre Boyer, et al [31]

"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."

From Dr I D Flintoff [32]

"As indicated in [2] narrow-band threat fields with simple modulations are no longer necessarily representative of the EMI which causes the failure in digital systems."

(Note: "narrow-band threat fields with simple modulations" is exactly how automotive radiated immunity testing is done.)

From IEC TS 61000-1-2, Ed 2, December 2008 [33]

"In most cases there is no simple or practicable way to check and to verify by means of testing or measuring that immunity is achieved for the safety-related system in its entirety with respect to other systems, equipment or the external electromagnetic environment for all operating conditions and operating modes."

"This is due to the fact that not every combination of operating conditions, of operating modes and of electromagnetic phenomena acting on the system can be achieved in a reasonable way and in a reasonable period."

For a detailed explanation of why EMC testing cannot be sufficient (i.e. on its own) to demonstrate that EMI in the operating environment cannot be a cause of unacceptable functional safety risks, read the first chapter in the IET's 2008 Guide.[34]

Notes

1. http://www.youtube.com/watch?v=KHGSWs4uJzY
2. The Norwalk Reflector, Feb 24, 2010 "Family's fatal outing becomes heart of Toyota controversy"
3. Gilbert, D.W., "Testimony for the Committee on Energy and Commerce, Sub-Committee on Oversight Investigations, Toyota Sudden Unintended Acceleration, February 23, 2010," http://energycommerce.house.gov/Press_111/20100223/Gilbert.Testimony.pdf
4. Hubing, Todd
   http://onlinepubs.trb.org/onlinepubs/ua/100701hubing.pdf
   http://www2.wspa.com/news/2010/jul/21/clemson-professor-studies-unintended-acceleration--ar-607687/
   http://cbs11tv.com/local/lexus.toyota.electronic.2.1826382.html
5. Regarding further issues of functional safety highlighted by this case: On this particular vehicle the ignition key – a "means of last resort" protection against a runaway vehicle – had been replaced by an ON/OFF push button that required to be continuously pushed for three seconds to operate. Further still, there remain questions as to

whether or not the electronic transmission control would allow the vehicle to be put into neutral at high speed – another “means of last resort”. It can be readily appreciated that had the design been subject to independent assessment at the design stage and a series of “what if?” and “worst case” scenarios had been worked through any functional safety deficiencies would have been identified and any necessary fail-safe measures and means of last resort would have been incorporated into the vehicle’s design.

6. http://www.nhtsa.gov/PR/DOT-54-10 U.S. Transportation Secretary Ray LaHood Announces Major Investigations to Resolve Issue of Sudden Acceleration, March 30, 2010
7. http://www8.nationalacademies.org/cp/projectview.aspx?key=49236
8. NHTSA’s own tests on a Lexus ES-350X (VRTC Memorandum Report EA07-010, VRTC-DCD-7113, 2007 Lexus ES350 Unintended Acceleration, April 30, 2008) show that at 50mph with its throttle jammed open, it took five times the normal maximum foot pressure on the brake to stop the vehicle in more than five times the normal distance. Many people may be unable to exert 130 pounds of pressure on the brake, and even if they could – five times the stopping distance cannot be considered “safely bringing the vehicle to a halt”. (Note that pumping the brakes – most drivers’ reaction to improve braking effectiveness – only makes things worse when the throttle is wide open, as it depletes the vacuum needed to provide brake power assistance.)
9. If an independent functional safety assessor had reviewed the Titanic, he would firstly have questioned the assertion of its unsinkability, secondly he would have imagined all possible scenarios involving an unsinkable ship sinking and thirdly, he would have made sure that the vessel had sufficient life boats and rafts installed to meet all possible emergencies. Under such a regime of independent assessment, the Titanic would not have been allowed to leave port on its maiden voyage until the assessor’s safety requirements had been met.
10. The IEC is the International Electrotechnical Commission, an international standards-creating body based in Switzerland. US experts play a very important part on IEC standards committees to which experts are appointed by all the developed nations. The World Trade Organisation (WTO) recommends that, to encourage trade globalisation, countries should adopt IEC standards as their national standards, as the USA, Canada and Europe mostly do already. http://www.iec.ch/functionalsafety
11. All seven parts of IEC 61508 were issued at Edition 2 in 2010.
12. EN 50128 “Railway Applications - Communications, Signalling and Processing Systems - Software for Railway Control and Protection Systems”
13. ISO is an international standards-creating organization, like the IEC: http://www.iso.org
14. Part of the reason for these deficiencies might be the very different approaches taken by the various national groups. A member of the ISO 26262 committee told one of the authors informally in 2008, that the Japanese appeared most interested in high-performance, the Europeans in safety for drivers and others, and the US in product liability issues. He said that several lists of things that could go wrong and should be taken into account during design had been truncated from 10 or more items to two or less, because US lawyers didn’t want to give plaintiff’s lawyers any clues as to how auto electronics might malfunction. Of course, this has degraded the effectiveness of the standard in insuring acceptable functional safety risks.
15. So unless there are significant changes we will “just have to take their word for it” that their vehicles actually comply with ISO 26262.
16. Faller and Goble, “Open IEC 61508 Certification of Products,” http://www.exida.com/articles/IEc%2061508%20Cerftification.pdf
17. Hubing, Todd, “Analysing Unintended Acceleration and Electronic Controls,” July 2010, http://onlinepubs.trb.org/onlinepubs/ua/100701hubing.pdf
18. NHTSA Investigation PE10008 Feb 18, 2010, 2009 Model Year Toyota Corolla. Summary: “THE OFFICE OF DEFECTS INVESTIGATIONS (ODI) HAS RECEIVED 168 OWNER COMPLAINTS WHICH ALLEGE EXPERIENCES WITH THE STEERING BECOMING UNRESPONSIVE OR LOOSE WHILE DRIVING AT HIGHWAY SPEEDS IN MODEL YEAR (MY) 2009 THROUGH 2010 TOYOTA COROLLA AND MATRIX VEHICLES EQUIPPED WITH ELECTRIC POWER STEERING. OF THESE, 8 ALLEGE THAT THE CONDITION CAUSED OR CONTRIBUTED TO A CRASH, INCLUDING 7 MAY 2009 VEHICLES AND 1 MAY 2010. A PRELIMINARY EVALUATION HAS BEEN OPENED TO ASSESS THE FREQUENCY, SCOPE AND SAFETY CONSEQUENCES OF THE ALLEGED DEFECT IN THE SUBJECT VEHICLES.”
19. EMC is the scientific and engineering discipline of ensuring that electrical/electronic technologies do not cause electromagnetic interference (EMI) due to their emissions of EM phenomena, and that they are also sufficiently immune to the EM phenomena occurring in their operating environment to function correctly.

20. IEC TS 61000-1-2, “Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena”. Edition 2 was published in December 2008, for a preview visit http://webstore.iec.ch/preview/info_iec61000-1-2%7Bed2.0%7Den.pdf.
21. From a report on a conference sponsored by the NATO Science Committee, Rome, Italy, 27–31 October, 1969, by J.N. Buxton and B. Randell, editors, Software Engineering Techniques, April 1970, p. 16. Believed to be the earliest documented use of this famous quotation, see http://en.wikiquote.org/wiki/Edsger_Wybe_Dijkstra
22. “The Quality Attitude,” News at SEI, March 1, 2004, http://www.sei.cmu.edu/library/abstracts/news-at-sei/wattsnew20043.cfm
23. “Software Testing,” Carnegie Mellon University, 18-849b Dependable Embedded Systems, Spring 1999, http://www.ece.cmu.edu/~koopman/des_s99/sw_testing
24. “Software Engineering, CST 1b,” http://www.cl.cam.ac.uk/teaching/0910/SWEng/cst-1b-sweng.ppt
25. “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
26. “Software Reliability,” http://swassurance.gsfc.nasa.gov/disciplines/reliability/index.php
27. “Computer Based Safety-Critical Systems,” September 2008, http://www.theiet.org/factfiles/it/computer-based-scs.cfm?type=pdf
28. “Analyzing Unintended Acceleration and Electronic Controls,” http://onlinepubs.trb.org/onlinepubs/ua/100701hubing.pdf
29. Tom Krisher, “Toyota’s Crisis Puts Spotlight on Auto Electronics,” Associated Press, Detroit, 25 February, 2010, http://abcnews.go.com/Technology/wirestory?id=9950797&page=4
30. “EMC Failures Happen,” Evaluation Engineering, December 2007, http://www.evaluationengineering.com/features/2007_december/1207_emc_test.aspx
31. “Characterization of the Evolution of IC Emissions After Accelerated Aging,” IEEE Transactions on EMC, Vol. 51, No. 4, November 2009, pages 892-900
32. “Preliminary Investigation into a Methodology for Assessing the Direct RF Susceptibility of Digital Hardware, Final Report for Radiocommunications Agency, Document No. R/99/042, Project No. 0921,” May 1999, http://www.ofcom.org/uk/static/archive/ra/topics/research/topics/emc/r99042/r99042.pdf
33. IEC TS 61000-1-2, Ed2, 2008: “Electromagnetic Compatibility (EMC) Part 1-2: General, Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena,” http://www.iec.ch/webstore
34. “EMC and Functional Safety,” the IET, August 2008, http://www.theiet.org/factfiles/emc/emc-factfile.cfm

Authors Note

All three of us provided the technical expertise for a press conference at the National Press Centre in Washington DC on March 23, 2010, explaining how automobiles may experience a dangerous loss of speed control as a result of EMI or software-related problems affecting their electronic throttle control and engine management systems, and making suggestions as to suitable preventive measures based upon what is already normal practice in other safety-related industries.

We will be pleased to provide more information if requested.

Dr Brian R Kirk BSc (Hons), MSc, PhD, MBCS, Chartered Engineer, MACM

Brian started working with computers in 1966 after gaining a BSc Hons (i.e. Cum Laudes) in Physical Electronics at Salford University followed by an MSc in Device Engineering, Processes and Computing at Imperial College and a PhD in Active Safety Systems in 2008.

His career started in the Microelectronics Industry with Marconi Research (UK) and then General Instrument Corporation (USA) where he was involved in the design and manufacture of microprocessors and custom chips. He was the Development Manager for Microprocessors and Memory Devices in the UK.

He became a founding Director of Robinson Systems Engineering Ltd in 1976 trading as Robinson Associates. The company specializes in designing and building high Integrity and safety critical embedded computing solutions, including safety critical systems for the Transport sector (some using the CAN bus).

Systems experience includes safety critical systems and software for Medical Equipment Automation, Railway Systems and Tools, Juridical Recorders' "Black Box" for Rail Systems, and an Active Safety "Black Box" for Aviation.

Brian is a Member of the British Computer Society (UK) and a life member of the Association of Computing Machinery (USA).

Dr. Brian R Kirk
Director, Robinson Associates
Weavers House, Friday Street Painswick, Gloucestershire, GL6 6QJ, UK
Tel: +44 1452 813 699 Fax: +44 1452 812912
Cell: +44 7785 354 365
E-mail: b.kirk@robinsons.co.uk
Web: http://www.robinsons.co.uk

Dr Antony Anderson PhD, BSc(Hons), Chartered Engineer, FIEE/FIET, FIDiagE

Since 1997 Dr Anderson has been working as an independent electrical consultant specialising in electrical machine and control system failure investigations and expert witness work. He has investigated a wide range of electrical/electronic related problems on behalf of various UK and US-based organizations in UK, France, Germany, Belgium, Mexico, Colombia and Canada.

He has investigated many issues, including: high speed stepper motor failures; switching transient problems in motor windings caused by pulse-width modulated inverters; electromagnetic bearing failures; mechanically induced EMI in generator rotors, and generator core failures.

Since 2000 he has also been investigating power electronics-related malfunctions in automobiles, including intermittent malfunctions of an electronic stability system and malfunctions in electronic speed control systems.

He has a BSc (Honours, i.e. Cum Laudes) in Electrical Engineering and a PhD (Electronic Control of Switched Reluctance Motors), both from the University of St Andrews, Queens College Dundee; Scotland, UK.

Previous experience includes: electronic control of rolling mill drives; simulation of variable speed drives; transient performance and stability of electrical machines; organizing superconducting machine design including minimization of effects of high strength rotating magnetic fields, screening etc; investigating transient electromagnetic field effects in large conventional a.c. machines.

He is a Fellow of the Institution of Engineering Technology (FIET) (formerly known as the IEE, Institution of Electrical Engineers, since 1871), a Fellow of the Institution of Diagnostic Engineers and a Member of the IEEE.

Dr Antony Anderson
Electrical Engineering Consultant
26 Westfield Drive, Gosforth, Newcastle upon Tyne, NE3 4XY, UK
Tel: +44 191 2854577 Fax: +44 191 2854577
E-mail: antony.anderson@onyxnet.co.uk
Web: http://www.antony-anderson.com

EurIng Keith Armstrong BSc(Eng)Hons, Chartered Engineer, FIET, SMIEEE, ACGI

Keith was awarded the BSc (Elec.Eng) with Honours (i.e. Cum Laudes) from Imperial College of Science & Technology, London, UK, in 1972, having specialized in electronic circuit design, control systems, and electromagnetic field theory.

He is a Group 1 European Engineer (EurIng), a Fellow of the Institution of Engineering Technology (FIET) (previously the IEE, since 1871), and a Senior Member of the IEEE.

His IEE/IET Fellowship and IEEE Senior Membership were awarded on the basis of his work since 1997 on the new discipline of "EMC for Functional Safety".
Keith has chaired the IEE/IET's Working Group on "EMC and Functional Safety" since 1997 and is the IET's official spokesperson on that topic.

He is the UK's expert on these International Electrotechnical Committee's teams:

IEC 60601-1-2 (EMC for safety of Medical Equipment and Systems)
IEC 61000-1-2 (Basic standard on EMC for Functional Safety)
IEC 61000-6-7 (Generic standard on EMC for Functional Safety

He has published the following books and is working on two more on EMI/EMC:
EMC for Printed Circuit Boards, Basic and Advanced Design Techniques, 2007, ISBN: 978-0-9555118-0-6
WMC for Systems and Installations (co-authored with Tim Williams), Newnes 2000, ISBN: 0-7506-4167-3

Since 1990 he has produced more than 191 papers, articles, guides and workshops in the USA, Europe and China, on EMI/EMC and "EMC for Functional Safety". Many have been translated by volunteers into Spanish, Chinese and Japanese (at their request).

Until 1990, Keith was employed in a number of industries as an electronic designer, later as project leader and design manager. Since 1990 he has been an Independent EMC and Safety consultant since 1990 with his own company, Cherry Clough Consultants, with over 700 customers in the USA, Canada, Europe and Asia.

As an independent he has solved a huge range of EMC problems in a wide range of industries and applications, from tiny products through systems of any complexity to large installations (e.g. synchrotrons) – including electronic modules for rail, aviation and automotive vehicles – and also provided very highly-regarded training courses on EMI/EMC and "EMC for Functional Safety".

EurIng Keith Armstrong
Cherry Clough Consultants
9 Bracken View, Brocton, Stafford, ST17 0TF, UK
Tel: +44 1785 660 247 Fax: +44 1785 660 247
Cell: +44 7785 726 643
E-mail: keith.armstrong@cherryclough.com
Web: http://www.cherryclough.com

Comments (2) **Search**

crichmond | Registered | 2010-11-09 09:28:46

Is this available to non-subscribers electronically? Despite its emphasis on automotive functional safety, it raises issues all compliance engineers and managers should be considering. I woud like to direct non-subscriber colleagues to a URL rather than losing my copy of INCompliance.

Regards,

Cortland Richmond

efeeney | SAdministrator | 2010-11-09 09:54:28

Yes, you can certainly share this article with a non-subscriber. At the top of this page, there is an e-mail icon to allow you to forward the information to your colleague.

Only registered users can write comments!