Another EMC resource
from EMC Standards

Absence of proof is not proof of absence

Helping you solve your EMC problems

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

Published in the EMC Journal, Issue 78, September 2008, pages 16-19, www.theemcjournal.com

Absence of proof is not proof of absence

(and the “proven in use” fallacy)

Keith Armstrong, Cherry Clough Consultants, www.cherryclough.com
As published in the Sept/Oct 2008 Edition of the EMC Journal (www.theemcjournal.com)

In my work in ‘EMC for Functional Safety’ over the last 10+ years, I have ventured out of the cosy world of electromagnetic (EM) compliance, where everything is done by EMC testing, into the ‘wild west’ of safety engineering, where affordable EMC testing can *never* be thorough enough to demonstrate that a design will be safe enough over its lifetime in its EM environment (see [1] [2] [3] [4]).

In the safety engineering world, I have often been told (and still am), even by the most senior executives and official regulators – who really ought to know better – that: “*We have no evidence that safety problems can be caused by electromagnetic interference.*” What they mean by this is: “*therefore there is no problem: EMI does not cause safety incidents”*.

This is one example of the fallacious “Absence of proof means proof of absence” argument, widely used by politicians, officials, and other people for whom perception is more important than reality. The purpose of this short article is to enable us to recognise and counter this type of spurious argument, wherever we meet it.

This incorrect argument is often used, or accepted, because it seems at first sight to be so self-evident that we do not think about its validity. But in safety engineering we have to be concerned with hard physical realities, so we must be able to recognise incorrect statements and false arguments – like this one – even where we *want* to believe them because they give us a warm and fuzzy *feeling* that everything is alright, or because they *appear* to justify cost savings.

It was William Cowper (1731 – 1800) who first wrote: "Absence of proof is not proof of absence" [5]. Unfortunately, even 200 years later, people who we trust to know better are still making this fundamental error.

The simple error in this argument, is the implicit assumption that the people making the statements have *actually tried to find any evidence*. We *assume* that they know what they are talking about, but often they do not. Simply because no one has told them that a specific problem has been found, they try to convey this to us as somehow meaning that therefore the problem cannot exist.

So the trick is – whenever someone tries to use the “absence of proof….” Argument – simply ask what actual grounds do they have for claiming proof of absence?

In almost all cases, their answer will reveal that there has been no attempt at a thorough investigation – often that there has been no investigation at all. The reason there is no evidence, is that nobody ever looked for any! Of course, having no evidence cannot prove anything at all, and so we can say, as William Cowper did over 200 years ago: "Absence of proof is not proof of absence".

Sometimes the reply is that an investigation has been done. But quite often it will be found not to have been a very thorough one, so do not be fobbed off by a reply like “Oh, we did an investigation” – ask to see the methodology and the resulting raw data. I have seen a government report in which the Executive Conclusions (written by an Official) stated that there was no evidence of a particular problem, despite being contradicted by the actual data (collected by an engineer)!

That the “absence of proof….” argument is fallacious, is well-known to top safety experts, and I quote from a few of them below. Prof. Henry Petrowski, writing in the New Scientist [6], gives

a number of real-life examples of engineering techniques that were “known” to be adequate – until their design flaws were eventually revealed at great cost.

He says [6]: “*Success frequently masks latent flaws in a design. The longer those flaws remain undetected – or telltale signs of them ignored – the more robust the evidently successful system will appear to be and it will tend to be pushed accordingly.*”

This also gives the lie to another common management approach to saving costs regardless of the true consequences for safety, which is known as ‘Proven in Use’. This might have been an acceptable rule in the 19th Century, but in our modern, complex, electronic age, it is just another variation of the fallacious “absence of proof means proof of absence” argument.

One of Prof Petrowski’s examples is the Columbia space shuttle disaster, of which he says [6]: “*Prior to 2003, virtually every space shuttle launch was accompanied by insulating foam being shed from its external tank. The fact that this caused no significant damage to the spacecraft put that kind of event in a category that did not halt flights.”*

“That all changed when Columbia suffered a critical breach in the leading edge of one of its wings. Because shedding foam had become a part of normal operations, Columbia was not sufficiently scrutinised before being cleared for re-entry in February 2003. Only its spectacular failure revealed incontrovertibly what some “overly cautious” engineers had been trying to warn NASA about.”

NASA management had assumed that because there was no evidence that chunks of foam hitting the space shuttle during launch had caused a problem, this “proved” that there was no problem with the space shuttle’s design. They never bothered to do a proper investigation, because the design of the space shuttle was considered to be “proven in use”. But when they bothered to do some actual investigations (*after* the Columbia disaster, naturally) they found that foam hitting the very brittle thermal tiles could in fact cause a catastrophe.

[6] concludes: “*It is in the public interest to recognise that the possibility of failure lurks in the dark corners and black boxes of technology, and that it is incumbent upon all those involved in design, construction and regulation to keep this fact high in their consciousness. None of us should become paranoid about engineering failures, but a healthy scepticism about built things, and an awareness that apparent success can mask imminent failure, should always inform those in charge of these structure’s condition and in whose hands rests the safety of the people who use them.*”

My first draft of this article included some of my experiences with the use of the “absence of proof….” argument, in the healthcare industry. My recent reading on Product Liability court cases reveals that lawyers, judges and juries tend to accept “absence of proof means proof of absence” and “proven in use” arguments, because they know no better, so the law is not providing the necessary corrections. Unfortunately, the article became too large so I have had to edit them out.

Now that we understand the underlying fallacies in the “absence of proof means proof of absence” types of argument, we can very quickly spot dubious politicians, officials and managers, and get annoyed by media reporters who don’t ask such people what hard, actual and meaningful evidence they have when they make such assertions.

Where people understand the fatal flaws in the “absence of proof…” argument, but use it anyway, they are trying to manipulate our perception. ‘Confidence trickster’ is a less polite description of such people. Where people actually believe what they are saying when they use such arguments, they should be trusted to about the same extent.

Now that we understand the fallacy in the “absence of proof means proof of absence” argument, the question then arises as to what we should do instead when trying to design high-technology products and systems so that they are safe enough.

If you thought that all that was necessary for making a product or system safe was to apply IEC/EN 60950 or IEC/EN 61010-1 or one of the many other published safety standards, then you need to get out more and update your understanding of safety engineering.

Almost all of these safety standards specifically do not cover safety risks due to malfunctions, for which a risk management approach is needed. Mostly, they just deal with 'inherent' safety issues such as electric shocks and fire hazards.

As electronic devices have become more complex over the years, and the modules and units they are used in, and the software they run, have also become more complex; as items of equipment have been increasingly interconnected to create systems and as systems are increasingly interconnected to create 'systems of systems'– the difficulty of ensuring that our electronic technologies do not introduce intolerable safety risks grows exponentially.

This increase in complexity means that we should not blindly assume that safety engineering techniques that used to work well enough, will continue to work equally well in the future. When technologies change, past experience is not necessarily a good guide to the future.

But in electronics, technologies are always changing. So even where an "absence of proof…" argument *is* correctly based on real and relevant data, it does not necessarily apply to the next project, because of its new technologies and increased complexity.

For example, a current development in automotive safety is the use of vehicle-to-vehicle wireless communications so that when vehicles meet a problem, they automatically control the speed of approaching vehicles that can't see the problem because they are around a corner, or in a fog. This is a complex system-of-systems, and because cars are consumer goods it will use lowest-cost technologies. Worried? You bet!

The necessary methodology to deal with complex devices, equipment and systems is known as Safety Risk Management, and I hope to write about it in a future article that will also discuss its relationship to – and the engineering reality behind – Murphy's Law.

In the meantime, I will leave you with some quotations from some more safety experts, relevant to the above issues.

From [7]: "New technology introduces unknowns into our systems and even unk-unks (unknown unknowns)"…….."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."…..."Digital technology has created a quiet revolution in most fields of engineering, but system engineering and system safety engineering techniques have not kept pace. Digital systems introduce new "failure modes" that are changing the nature of accidents. Many of the approaches that worked on electromechanical components – such as replication of components to protect against individual component failure (i.e., redundancy) – are ineffective in controlling accidents that arise from the use of digital systems and software."……."This situation is not new: Throughout history, inventions and new technology have often gotten ahead of their scientific underpinnings and engineering knowledge, but the result has always been increased risk and accidents until science and engineering caught up."

From [8], using slightly more academic language: "Implicitly, safety engineering assumes that probabilities reflect aleatoric uncertainty, i.e. 'randomness', which can be characterised by a stochastic model. Further, we implicitly assume ergodicity – that past failure behaviours are good predictors of the future. ….. However, in many cases we face epistemic uncertainty, i.e. imperfect knowledge of the system or the stochastic model. In other words, we do not know the shape of the probability density function (PDF) or even its mean."

[1] "*Why EMC Immunity Testing is Inadequate for Functional Safety*", Keith Armstrong, 2004 IEEE International EMC Symposium, Santa Clara, USA, August 9-13 2004, ISBN 0-7803-8443-1, pp 145-149. Also published in Conformity, March 2005 pp 15-23, http://www.conformity.com.

[2] "*Functional Safety Requires Much More Than EMC Testing*", Keith Armstrong, EMC-Europe 2004 (6th International Symposium on EMC), Eindhoven, The Netherlands, September 6-10 2004, ISBN: 90-6144-990-1, pp 348-353.

[3] "*EMC in Safety Cases — Why EMC Testing is Never Enough*", Keith Armstrong, EMC-UK 2007 conference, Newbury, UK, Defence & Avionics session, Wednesday 17th October 2007.

[4] "*Why EMC Immunity Testing is Inadequate for Functional Safety*", Keith Armstrong, 2008 IEEE International EMC Symposium, Detroit, USA, August 18-22 2008, ISBN 978-1-4244-1699-8. A longer version of this paper is being serialised in five parts by Automotive Design Europe, www.automotivedesign-europe.com.

[5] Antony Anderson, presentation to the 20th Conference of the Society of Expert Witnesses, Alexander House, Wroughton, 16th May 2008, www.sew.org.uk. Antony is a forensic engineer and expert witness, antony.anderson@onyxnet.co.uk.

[6] "*When Failure Strikes*", Henry Petrowski (Alexandar S. Vesic Professor of Civil Engineering and a Professor of History at Duke University, NC, USA) New Scientist, 29 July 2006, page 20. Also at: http://www.newscientist.com/channel/opinion/mg19125625.600-the-success-that-allows-failure-to-strike.html.

[7] "*A New Accident Model for Engineering Safer Systems*", Nancy Leveson (Professor of Aeronautics ands Astronautics, Massachusetts Institute of Technology, MIT, Boston, USA), Safety Science, Vol. 42, No. 4, April 2004, pp. 237-270, http://sunnyday.mit.edu/accidents/safetyscience-single.pdf. Ms Leveson's biography is at http://sunnyday.mit.edu.

[8] "*Risk, Uncertainty, Software and Professional Ethics*", John McDermid (Professor of Safety Engineering at the University of York, Head of the Department of Computer Science, Head of the High Integrity Systems Engineering Group, and an Independent Safety Assessor), Safety-Critical Systems Club Newsletter, January 2008, Volume 17 No. 2, pp 5-8, http://www.safety-club.org.uk/main.html?opt=Publications