Another EMC resource
from EMC Standards

Why Do We Need an IEEE EMC Standard on Managing Functional Safety and Other Risks? IEEE EMC Mag 2016

Helping you solve your EMC problems

1 Brassey Road, Old Potts Way, Shrewsbury, SY3 7FA T:+44 (0) 1785 660 247 E:info@emcstandards.co.uk

Why Do We Need an IEEE EMC Standard on Managing Functional Safety and Other Risks?

Keith Armstrong, Cherry Clough Consultants,
www.cherryclough.com www.emcstandards.co.uk, October 2018

This is an updated version of a paper first published in the IEEE EMC Magazine, Volume 5, Quarter 1, June 2016: "Why Do We Need an IEEE EMC Standard on Managing Risks?"

Most of our EMC industry appears to think that immunity testing to traditional standards covers everything that is needed regarding protection from EM disturbances, and – if there are safety issues – just double the test levels to create a (*so-called*) "Safety Margin"!

If the safety issues are very critical indeed, then triple or quadruple the test levels to…..well, I'm sure you get the picture.

After 20 years of working on this issue, 17 years of presenting IEEE conference papers on it, and 13 years on the two most relevant IEC EMC/safety standards teams, I think I can now explain – using three simple arguments – why the IEEE's EMC Society felt the need to create the first of a new *type* of EMC standard: "**Techniques and Measures to Manage Functional Safety and other Risks with Regard to Electromagnetic Disturbances**".

1 The Problem of the Low Risk Level and the EM Environment

Functional safety risk levels are measured in parts-per-million (ppm) per person per year, with the UK's Health and Safety Executive (HSE, www.hse.gov.uk) requiring a cost/benefit analysis based on the value of the lives saved by improving the design if the risk of death exceeds 1ppm/person/year during the anticipated lifecycle.

In any safety-critical electronic system there are many possible contributors to each dangerous failure, so the risks due to EM disturbances alone are generally set at $1/10^{th}$ of the overall risk target. For example if the risk of death target is 1ppm/person/year then the target for the risk due to EM disturbances alone would generally be set at 0.1ppm/person/year. Because EMI causes systematic failure modes (rather than random) this means we need to achieve a "design confidence" that EM disturbances will not cause a person to be killed in a year, of 99.99999%.

Some of the most dangerous occupations in the world have been estimated by the HSE to have risks of death around 1000 ppm/person/year, and following the usual method we would allocate a risk target of 100 ppm/person/year for the EM disturbances alone. That is, a design confidence of 99.99%.

Now let's compare this with our confidence in knowing the real-life EM environment of any system for the next year.

The normal EMC immunity test standards, for example as listed under the EMC Directive, are claimed to cover 80-95% (depending on the standards team members one talks to) of the typical daily/weekly EM disturbances in a typical application. But even 95% confidence in setting a test level is a far cry from the 99.99% to 99.9999% range we would require if we wanted to rely on EMC testing alone to help prove a system was safe enough.

Also, because they only cover *typical* daily/weekly EM disturbances, the effects of lightning and other rare EM disturbances (e.g. an insulation failure in a nearby equipment causing a fuse to open) are excluded, although we would have to take them into account in our immunity testing because we have to ensure acceptable safety risk levels for the whole lifecycle.

(I still don’t understand why the traditional immunity standards don’t cover the very close proximity (i.e. closer than 25mm) of cellphones and other personal electronic devices containing low-power radio transmitters, which is now a commonplace situation and – due to the Internet of Things(IoT) – will soon become ubiquitous.)

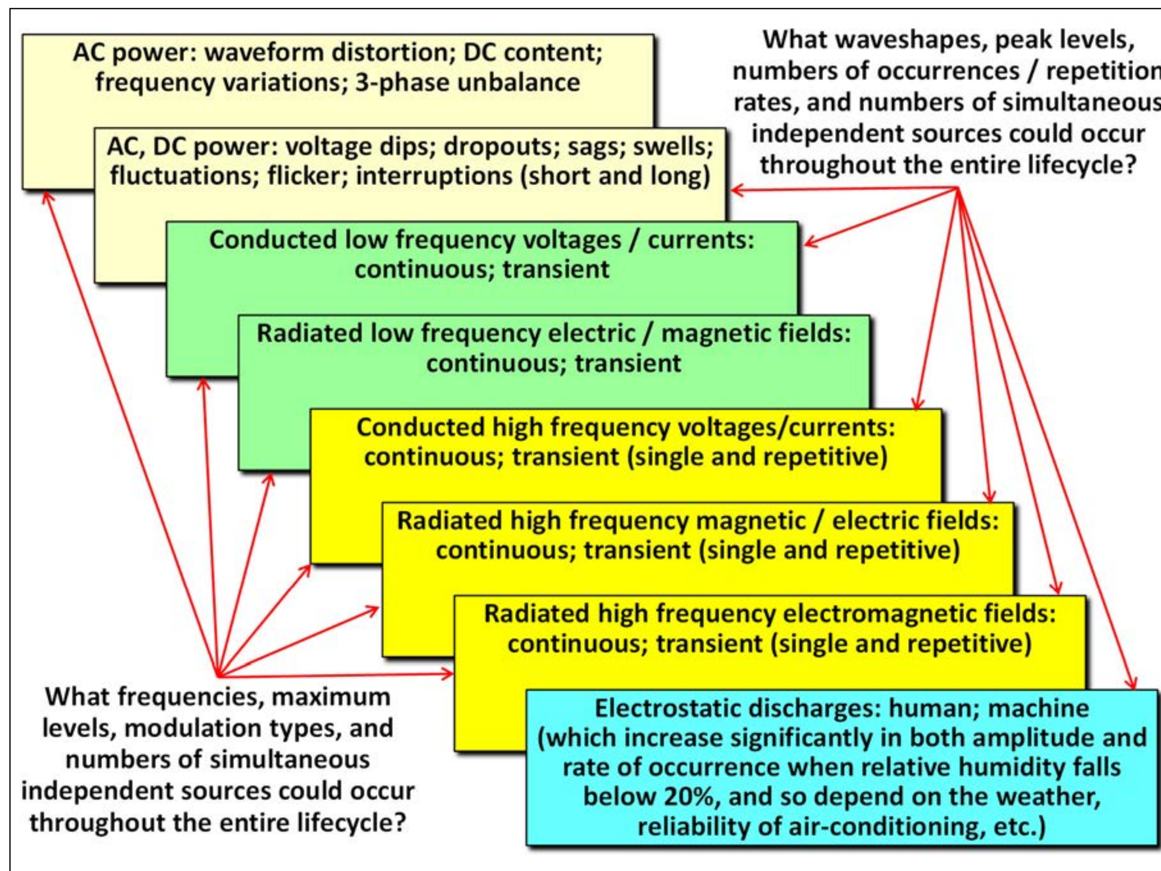

Figure 1 The problem of predicting the future EM environment with sufficient accuracy for managing risks measured in ppm/year

Some industries (notably the military) specify EMC immunity test standards based on their measurements of their EM environments, including lightning and other rare or unpredictable EM disturbances – but even they would surely balk at claiming their standards covered even 99.99% of a specified EM environment for even a few months.

In the next few years alone we can confidently expect many general changes to EM environments, all of them making it worse (of course). For example, the roll-out of 5G cellphone systems is expected to be underway by 2020, but we still don't know what frequency ranges, modulation types and RF power levels it will employ, or how close the basestations will be to each other. Also, switching power converters will operate at frequencies 10 to 100 times faster due to the use of Silicon Carbide or Gallium Nitride devices, making them noisier at much higher frequencies. They will also become significantly smaller in size, cost less, and dissipate less heat, which considerably increase their use in many applications, including all types of domestic appliances.

I could go on.....but it is clear that we simply can't know – even to the confidence levels acceptable for the world’s most dangerous occupations – what types of EM disturbances we should test for, and the test levels to use.

2 The Problem of the Untestable Number of Digital States

For at least 30 years it has been impossible to test more than a tiny fraction of all the possible digital states that a microprocessor could get into. Some of us will remember the error in the floating point calculation in the Pentium IV, which arose because it wasn't tested due to lack of time.

It is the same situation for testing all the possible digital states that a software program could get into. I understand that the state of the art in 2013 was that the largest software company in the world could now fully test a.........(wait for it!).........Printer Driver!

Even with the fastest test system in the world, fully testing many microprocessors or software programs would require millions of years! Possibly billions.

When testing linear electronic systems, once a suitable percentage of possible states have been tested we can be confident in predicting the behaviors of the untested ones. Unfortunately, all digital systems are non-linear, which means that even if we could test 99% of all their possible states – which we can't – we *still* couldn't extrapolate those results to provide any reliable information about the remaining 1% of untested states.

One result of this, is a well-known problem of most digital systems– they can fail in an unpredictable manner as the direct result of untested combinations of *perfectly correct* inputs!

> For example, if a digital system had four inputs each digitized to just 8-bit accuracy plus sixteen binary inputs (either on or off), and all inputs were independent of each other, there would be 2^{41} possible combinations of correct inputs, slightly more than $2{\cdot}10^{12}$. At 100 nanoseconds per test it would take $2{\cdot}10^{5}$ seconds to test them all – about 2.3 days, if testing 24/7.

Of course, there are many more possible system states than are required for just the "input space", not least to handle the processing of the data, and to discover whether EMI could cause an unsafe error or malfunction by immunity testing alone, we would need to apply each EMC test in turn to all possible system states.

> However, limiting our example to the input space alone, when performing a radiated immunity test (e.g. to IEC 61000-4-3) we would first set the lowest frequency at the correct level (taking measurement uncertainty into account, of course) then dwell at that frequency while going through the complete set of correct input states. For the simple system discussed above, this would of course take 2.3 days (24/7).
>
> Then we would step to the frequency 1% higher and do the same, dwelling for another 2.3 days. After about 230 steps taking nearly 1.5 years we would finally reach a decade higher in frequency. Then we would repeat this with three other angles of incidence, and then repeat the whole lot yet again with 90° antenna polarization.
>
> So even the simple example system discussed earlier would need about 12 years of 24/7 immunity testing to perform an IEC 61000-4-3 test covering just one a decade of frequency, on its "input space" alone.

But we will usually need to do cover more than one decade of frequency, and we have other types of EM disturbances to test as well, some of which might require similar time-spans. If we assume we could test all the digital states we needed to in just 5 days, and planned to test conducted RF immunity on two cable ports from 100kHz to 100MHz; radiated disturbances from 100MHz to 10GHz; EFT/B at four test levels on one cable, and ESD on 10 test points with four test levels, we would probably need about 58 years of 24/7 testing.

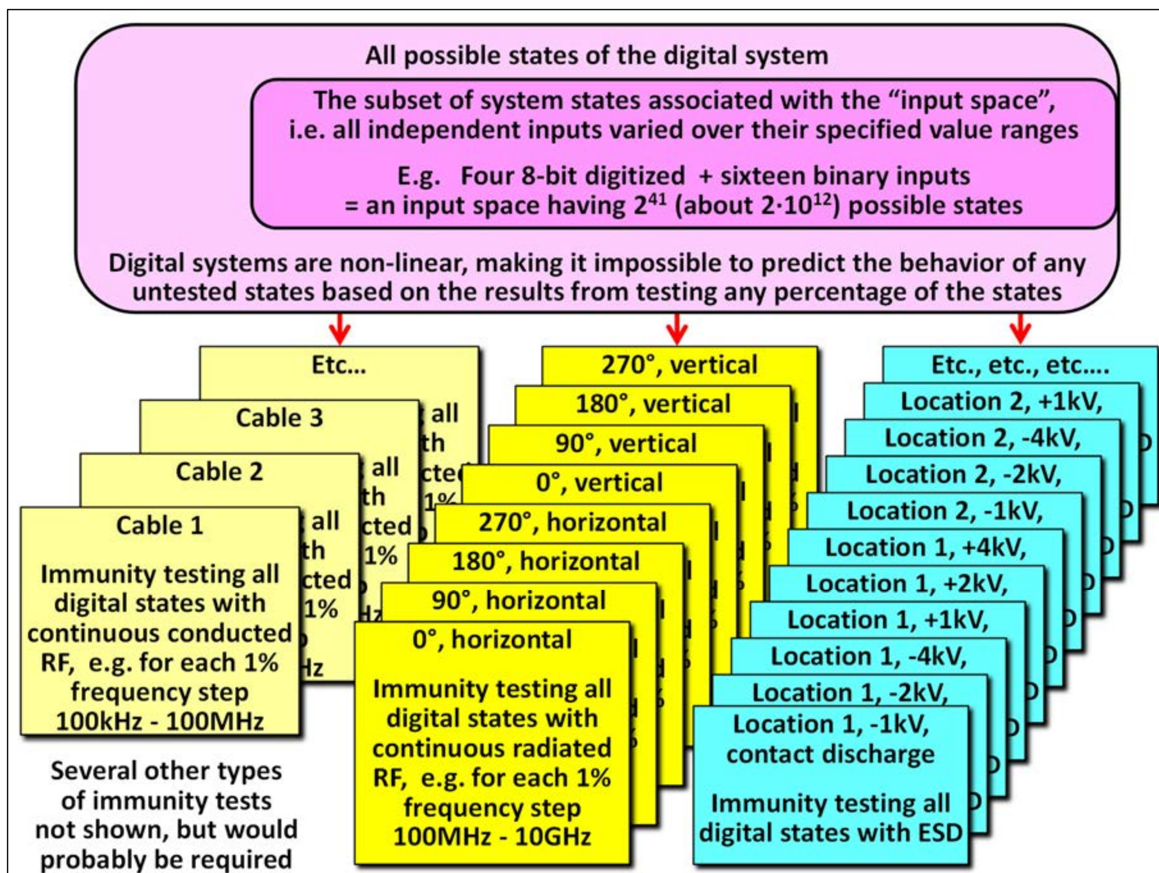

Figure 2 The problem of testing a sufficient number of digital states to manage risks which are measured in ppm/year

Of course, this is all a gross simplification! If we assume we could use "intelligent" digital testing techniques to reduce the number of states to be tested by 10 (without, of course, compromising our design confidence of between 99.99% and 99.99999%), our simple example system could be EMC tested in about 6 years.

However, the above example is possibly unrepresentative of future mass-produced safety-related systems, such as the one described in the following quotation from NVIDIA: *"Self-driving cars use a broad spectrum of sensors to understand their surroundings. DRIVE PX 2 can process the inputs of 12 video cameras, plus lidar, radar and ultrasonic sensors. It fuses them to accurately detect objects, identify them, determine where the car is relative to the world around it, and then calculate its optimal path for safe travel."* (Visit https://www.nvidia.com/en-au/self-driving-cars/drive-px/)

If we assume the DRIVE PX 2 to have eighteen 8-bit digitized inputs (and monochrome cameras), it would have 2^{144} possible input states, which is 2^{103} more than the worked example above. Even with "intelligent" digital testing techniques giving a 10:1 reduction and if we could somehow get the digital state testing time down to just 10 nanoseconds, testing its input space alone with just one radiated frequency, one angle of incidence and one antenna polarization would need a dwell time of more than $6{\cdot}10^{26}$ years (24/7) – about $4{\cdot}10^{16}$ times the age of the universe.

Of course, these examples are crude in the extreme, but they show that it is totally impractical to use immunity testing alone to demonstrate that EM disturbances should not create unacceptable functional safety risks, for all but the *very* simplest digital systems.

3 The Problem of the Exploding EMC Test Plan

We need to achieve a design confidence of between 99.99% and 99.99999% over the entire lifecycle of a system, so if we *assume for the sake of argument* that problems 1 and 2 above have been dealt with, we would still have to perform the suite of EMC tests many times to simulate the likely consequences of the following real-life situations:

a) Reasonably foreseeable degradations and failures in each EMC-significant component or connection (e.g. connector pins, solder joints, etc.), throughout the entire lifecycle. For example, caused by: initial tolerances; aging; corrosion; use and/or misuse; wear; misassembly; counterfeit parts; temperature/pressure/humidity coefficients, and more.

b) Foreseeable real-life EM disturbances in the system's intended operational environment that varied significantly enough from the traditional immunity tests (e.g. modulation type/frequency, transient waveshape and/or repetition rate, etc.) to warrant additional immunity tests.

c) Foreseeable combinations of the degradations and failures in a) above during the anticipated lifecycle, plus foreseeable combinations of independent real-life EM disturbances in b) above during the anticipated lifecycle, for example: two or more radiated fields at different frequencies (any frequencies); a radiated field at any frequency plus an ESD event at any location at any voltage; a radiated field at any frequency plus a fast transient burst at any voltage; a supply voltage at the low end of its tolerance plus harmonic distortion that reduces its peak height, plus a dip, dropout or short interruption, etc.

d) Foreseeable combinations of a), b), and c) above, during the anticipated lifecycle. (After all, they are mostly independent variables.)

It very quickly becomes obvious that trying to cover all these reasonably foreseeable situations over the lifetime would create a "test plan explosion". Even if a digital system could possibly be EMC tested to the appropriate level of design confidence in the 3 years mentioned above, and even if we assumed that only 10 sets of tests were needed to simulate a) above; a further 10 sets were required to cover b), and 100 tests required to cover c), we would have to repeat the standards immunity tests 120 times to demonstrate that the electronic system we were testing would be safe enough over its anticipated lifecycle.

Even if we could afford the huge testing cost, we simply couldn't wait that long for the test results!

4 The Problem that EMC testing Does Not Simulate Real EM Environments Well Enough

This 4th argument would also raise its ugly head if we were seriously trying to use immunity testing alone to achieve between 99.99% and 99.99999% confidence that EM disturbances that could occur during the lifecycle would not cause unacceptable risks – but I have run out of space in this brief article.

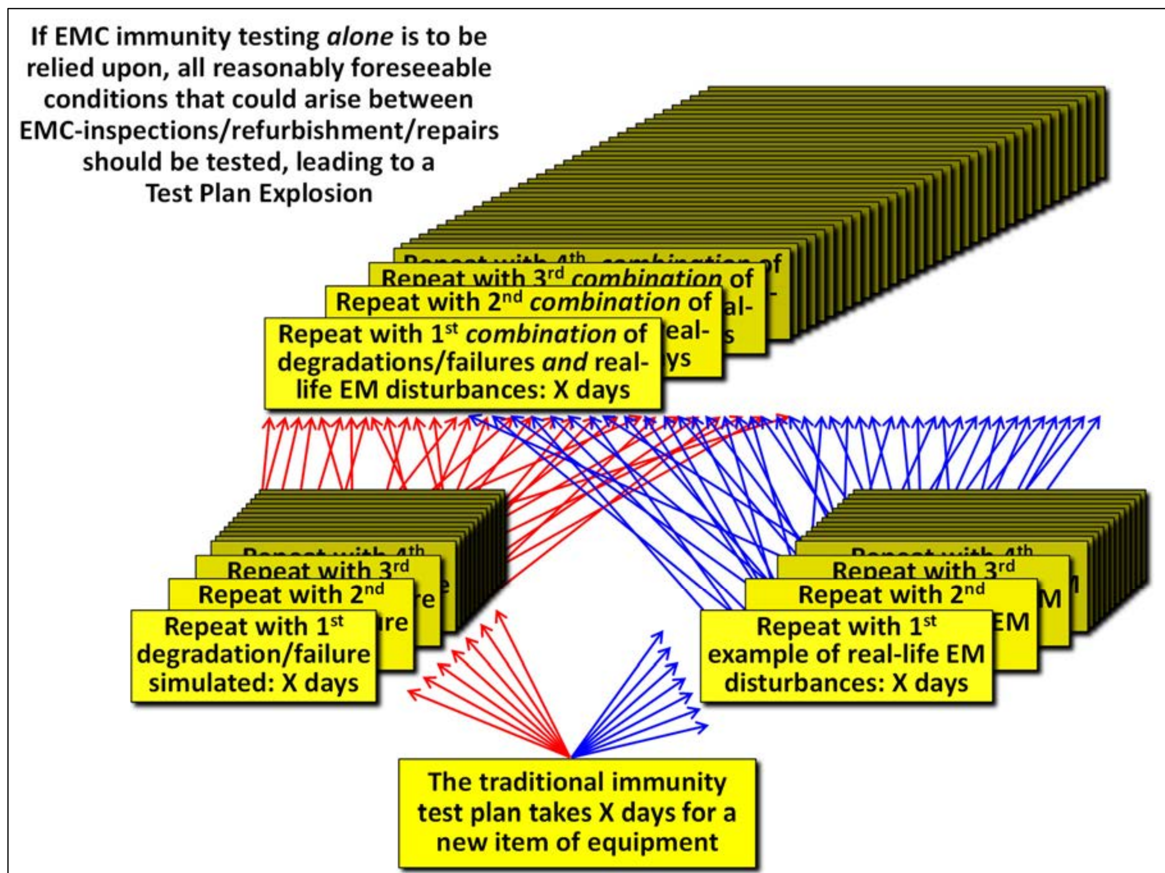

Figure 3 The problem of the exploding test plan

5 So, What *Should* We Do, In Practice?

The military have dealt with all the above problems by installing their safety-critical systems inside high-specification EM-mitigating (shielding, filtering, surge/transient suppression, fiber-optics, power supply backup, etc.) enclosures that are sufficiently rugged not to lose too much of their mitigation's performance between maintenance intervals. As there seems to be no widely recognized name for this traditional approach, I have taken to calling it the "Big Grey Box" (BGB) method.

Unfortunately, the BGB method it is often considered to be too large, heavy or costly, or too dependent upon regular maintenance, for many modern safety-related systems using digital electronics.

To deal with the inability to test all of the states of a modern digital system, industry and academia worldwide worked together for about 20 years to create IEC 61508, first published in 2000. This "Basic IEC Safety Publication" is effectively a collection of well-proven practical techniques and measures for use in the design, verification, validation and independent assessment of functional safety-related systems.

61508's design techniques and measures essentially detect errors, malfunctions or failures in signals, data and power supplies which could cause an unacceptable level of risk – in real-time, during operation. When such a problem is detected, it is either corrected or the system is switched into a "safe state" quickly enough that safety risks are kept within acceptable levels.

These design techniques and measures include: error detection / correction coding of data; redundant channels with comparison or voting; redundant power supplies, and a range of other

techniques which which many designers have been very familiar with since well before IEC 61508 was first published in 2000.

EMI actually means the errors, malfunctions or failures occurring in signals, data or power supplies as the result of EM disturbances, which means that many of IEC 61508's techniques and measures are quite effective at dealing with it.

The upcoming new IEEE Standard P1848 on "**Techniques and Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetic Disturbances**" will describe the Big Grey Box approach then go on to provide an alternative – identifying which of IEC 61508's practical techniques and measures should be used in design and its verification and validation, what modifications they might need, and what new techniques and measures may also be required, to ensure that acceptable safety risk levels will not be exceeded by any reasonably foreseeable EMI over the lifecycle.

This alternative approach effectively means that any EMI which occurs because of EM disturbances outside the tested parameters (see problem 1 above), or because of any of the issues discussed in 2, 3 and 4 above, is detected by the system itself. If it could increase safety risks above acceptable levels, its effects are either corrected or the system is switched into a safe state.

All the work on this subject has been focused on functional safety risks, but the same techniques and measures can also be used to manage any other kind of risk (e.g. financial risk) – as long as the type of risk is identified and an acceptable level specified.

For further information and to answer questions, or to join the IEEE P1848 Working Group, please contact the author Keith Armstrong, on keith.armstrong@cherryclough.com.

Bio for Keith Armstrong

Keith graduated from Imperial College, London, in 1972 with an Honours Degree in Electrical Engineering. He has been a member of the IEE/IET since 1977 and a member of the IEEE since 1997. Appointed IET Fellow and IEEE Senior Member in 2010.

After working as an electronic designer, project manager then design department manager, Keith started Cherry Clough Consultants in 1990 to help companies reduce financial risks and project timescales through the use of well-proven electromagnetic engineering design techniques.

Keith has chaired the IET's Working Group on EMC and Functional Safety since 1997 and is the UK's appointed expert to the IEC committees on:
IEC 61000-1-2 (the basic standard on EMC for Functional Safety);
IEC 61000-6-7 (generic standard on EMC for Functional Safety); and,
IEC 60601-1-2 (risk management of EMC for medical devices).

Since 2015 he has chaired the IEEE Standards P1848 team creating: "*IEEE Standard Practice for Techniques and Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetic Disturbances*".