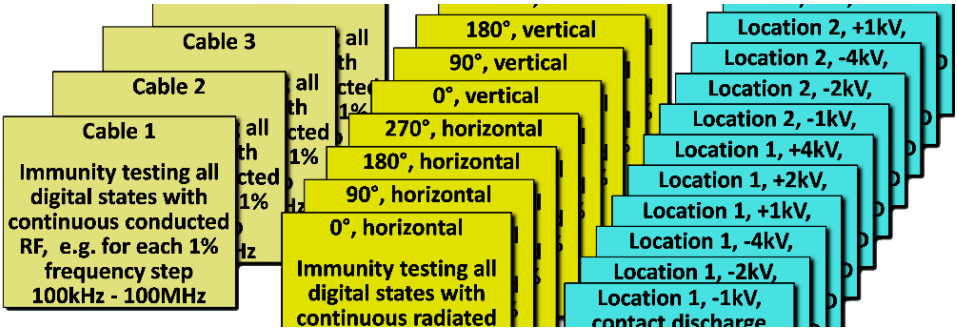
Why do we need new standards for EMI Functional Safety Risks?



In this first of a series of articles focusing on Electromagnetic Interference (EMI), Keith Armstrong and Davy Pissoort discuss the challenges associated with managing EMI Functional Safety Risks and present the case for the need for further standardisation.

All electronics can be upset by electromagnetic (EM) disturbances, causing electromagnetic interference (EMI), so the functional safety risk management process should take EMI into account.

It is widely, but incorrectly thought that Electromagnetic Compatibility (EMC) testing covers everything that can go wrong, and all that is needed for managing Functional Safety is to increase immunity test levels to create a (*so-called*) "Safety Margin". This pervasive myth was debunked in 2004 [1] and again in [2], but it still seems to be very widespread, so it seems appropriate to reiterate why no amount of immunity testing can possibly demonstrate that a digital system has low-enough risks from EMI for typical Functional Safety applications, whatever the immunity test levels used.

"For at least 30 years it has been impossible to test more than a tiny fraction of all the possible digital states"

It is impossible to test all digital states even once

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 and its software can get into, see [4] [5] [6] and [7]. We understand that, in 2013, the largest software companies in the world could only perform 100% state testing on printer drivers. Even with the fastest test system in the world, fully

testing many microprocessors or software programs would require millions, or possibly billions, of years.

Linear electronic systems can extrapolate from the results of testing a percentage of their possible states, to predict the behaviours of their untested states. But all digital systems are *non-linear*, which means that even if it was possible to test 90% of all their possible states (which it isn't), the results could never be extrapolated to predict the behaviour of the 10% that were not tested, see [8].

The digital industry has known for decades that their systems can fail in unpredictable ways as the direct result of untested combinations of *perfectly correct input*s, [9]. For example, if a digital system had four inputs, each digitized to 8-bit accuracy, plus 16 binary inputs (e.g. switches: either on or off), and if all inputs were independent of each other, there would be 2^{48} possible combinations of correct inputs, about $2.8 \cdot x\ 10^{14}$.

At 100 nanoseconds (ns) per input state test it would take $2.8 \cdot x\ 10^{7}$ seconds to test them all - about 326 days of testing 24/7, and of course, there are many more system states than are required for just the "input space", not least to handle the processing of the input data.

To discover whether EMI could cause an unsafe error or malfunction by immunity testing alone would require a large number of EMC tests to be applied in turn to all possible system states.

If we limit our example to the input space alone, when performing a radiated immunity test (e.g. to IEC 61000-4-3) the lowest frequency would be set at the correct level (taking measurement uncertainty into account), and the test would dwell at that frequency while the complete set of correct input states was exercised.

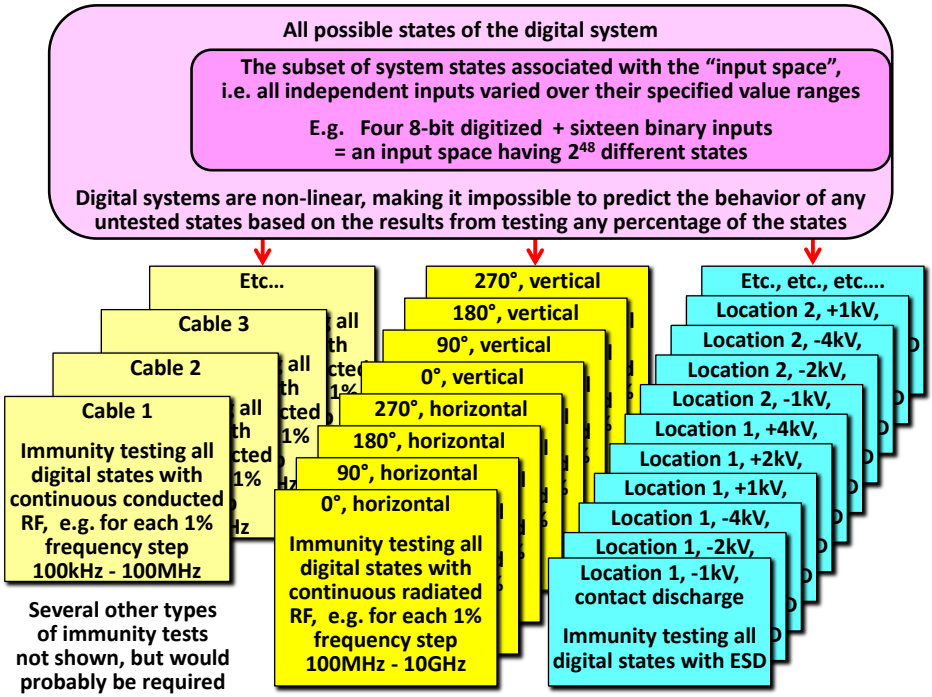
"A very simple immunity test plan would require a mere 5,000 years just to test the input state space"

For the simple example system above, this would take 326 days. Then the test frequency would be stepped 1% higher for another 326 days, and repeating this 230 times would cover the first *decade* of frequency (e.g. from 10 MHz to 100MHz), taking about 207 years of testing 24/7/365 to test just one decade of frequency with one angle of incidence and one antenna polarization!

Of course, this is all a gross simplification: it might be possible to reduce the testing time; and it might also be possible to speed up the testing of the system states. So let's assume that "intelligent" digital testing techniques reduce the number of states to be tested by 10 (without, of course, compromising the design confidence we need for SILs 1-4).

Let's also assume that each digital state can be tested in 1 ns instead of 100 ns. In this case, the very simple immunity test plan in the figure would require a mere 5,000 years just to test the input state space for this simple example system.

The idea of using immunity testing alone to prove a system is safe enough as regards EM disturbances, is clearly not viable.



Future mass-produced safety-related systems, such as those intended for autonomous cars, can be a lot more complex than the simple example shown. Assuming the DRIVE PX 2 [10] to have eighteen 8-bit digitized monochrome camera inputs, it would have 2144 possible input states, 296 times more than the simple worked example above.

The Near-Future EM Environment

The level of design confidence required for the desired SIL should be compared with the lack of confidence in knowing what the real-world EM environment of a system will be, over its entire lifecycle.

EMC immunity test standards, such as those listed under the European Union's EMC Directive, are claimed to cover 80-95% (depending on which standards' team member one talks to) of the typical daily/weekly EM disturbances in a typical application.

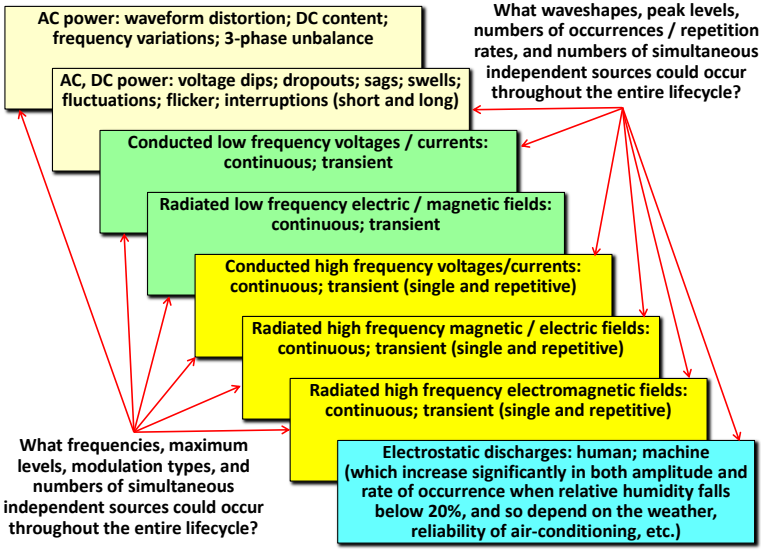
But even 95% confidence in setting a test level is a far cry from the 99.99% or better (for SIL1), required to help prove a system was safe enough. Also, these standards only cover typical daily/weekly EM disturbances, and ignore the effects of rare EM disturbances, even when they could be expected to occur during a typical lifecycle.

We also fail to understand why these test standards *still* do not cover the very close proximity (e.g. closer than 50mm) of cellphones and other personal electronic devices containing low-power radio transmitters, even though this is now a commonplace situation, and with the Internet of Things (IoT) will soon become ubiquitous.

In the next few years alone, the following general changes to EM environments are confidently expected:

- 5G cellphone systems with 100-times the data bandwidth of current benchmarks are expected to begin rolling out in 2020, but their frequency ranges, modulations and RF power levels, and how close the basestations will be to each other, are still unknown.
- Switching power converters will operate at frequencies 10 to 100 times faster due to the use of Silicon Carbide or Gallium Nitride devices, significantly reducing their size, cost and waste heat. This will in turn increase their use in many more applications, including all domestic appliances. Unfortunately, switching faster will also make them much noisier, at much higher frequencies.
- LED lighting will replace most incandescent and fluorescent lighting, using switching power converters that are much noisier than those technologies.
- Wireless Power Transfer (WPT) will use switching power converters to generate magnetic fields to charge the batteries in devices from cellphones to automobiles, trucks, buses, and trams at up to 22kW, with as much as 50% of these noisy fields "leaking" into the environment. Close proximity to WPT chargers will expose devices to intense fields, and it is impossible to ensure that this cannot happen.
- The use of PowerLine Telecommunications (PLT), sometimes called Broadband over PowerLine (BPL) is increasing, with ever-higher data rates.
- The use of Radio Frequency Identification (RFID) is increasing, with powerful fields generated near to their fixed or mobile readers.
- Machine-to-Machine (M2M) wireless data communications is expected to increase dramatically due to so-called Industry 4.0 and the IoT [11].
- Automobile safety systems will increasingly use steered radar beams of a few watts at frequencies including 76GHz, and modern silicon devices at 7nm or less are susceptible to such frequencies. Autonomous road vehicles may rely on several such radars, not just a single 'active cruise control' radar.
- AC electrical power networks will increasingly suffer harmonic and interharmonic waveform distortion/noise as linear loads continue to be replaced by non-linear loads such as the rectifiers in switching power converters. They will also suffer increasing levels of distortion due to the rapid increase in connections of AICs (active infeed converters), which convert the electrical power generated by photovoltaic panels/arrays, wind or water turbines, and other 'green' energy sources into a form suitable for feeding into mains power networks.
- Software-controlled radio will make better use of the limited radio spectrum by filling up any "empty" slots in the spectrum. The radio spectrum will eventually be entirely filled with frequency-hopping transmissions, for most of the time.

It is clear that even if immunity testing was practicable, it would be impossible to have any confidence in the types of EM disturbances or their test levels that should be used to be able to demonstrate that EMI should not cause unacceptably high risk levels during a lifecycle. The figure shows graphically, the problem of trying to predict the future EM environment with sufficient accuracy.



Real EM Environments are not simulated well-enough by EMC test standards

EMC test methods are designed for accuracy, repeatability, and low cost – and therefore do not necessarily simulate real life very well. For example, most radiated EM field immunity testing is done in anechoic chambers that create an environment unlike any real-life situation (other than an aircraft or missile in free flight). In real life there will be one or more surfaces reflecting EM fields from a variety of angles. The waveforms used for fast transient burst, surge and electrostatic discharge testing are very simplified versions of the real-world EM disturbances they are supposed to represent.

In some cases, the test waveforms are defined by what test equipment can be manufactured at an affordable price. For example, fast transient burst (FTB) testing uses pulses with fixed amplitudes and a repetition rate of either 5kHz or 100kHz, whereas, the EM disturbances from the electro-mechanical contacts that the FTB test is intended to represent actually varies in frequency from MHz to kHz as the contact gap opens, with a rising amplitude as the frequency decreases.

Another example is in electronic warfare and munitions where EMC experts know that when an RF 'threat' is modulated at a frequency corresponding to the rate of electrical activity in the target equipment, the target's susceptibility (vulnerability) increases dramatically.

Real-world sources of RF interference have a huge possible range of modulation frequencies, but normal immunity testing (using IEC/EN 61000-4-3 and IEC/EN 61000-4-6) uses only 1kHz sine-wave modulation, while military and some other standards use 1kHz pulse-modulation; neither of which is certain to discover all possible responses of the tested equipment to real-life RF threats.

One of the authors has been involved with two situations where equipment passed tests with any 1kHz sine-wave modulated radio frequency at up to 100 V/m, but were at least 80 dB more susceptible (i.e. would only take up to 10 millivolts/m) when the modulation frequency was set to their circuit's operating frequency. Both of these situations were discovered by accident, and both would cause severe financial and/or safety problems if interference occurred during normal operation.

Ref [12] makes the point that normal testing standards can give an erroneous impression of an equipment's EM performance in real life, due to the effects of load and temperature variations upon the inductors used in EMI filters; it gives an example of a mains supply filter's performance that fell by 20dB when operated at its rated maximum continuous voltage, current and temperature.

The Exploding EMC Test Plan

Assuming that all the issues discussed above have *somehow* been dealt with (although they cannot), the immunity tests would have to be performed many times to address the following real-life situations:

a) Reasonably foreseeable degradations and failures in EMC-significant components or connections (e.g. connector pins, solder joints, filter ground connections, etc.), throughout the lifecycle. These could be caused by: initial tolerances, aging, corrosion, use/misuse, wear, mis-assembly, temperature/pressure/humidity, vibration, shock, etc.

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.

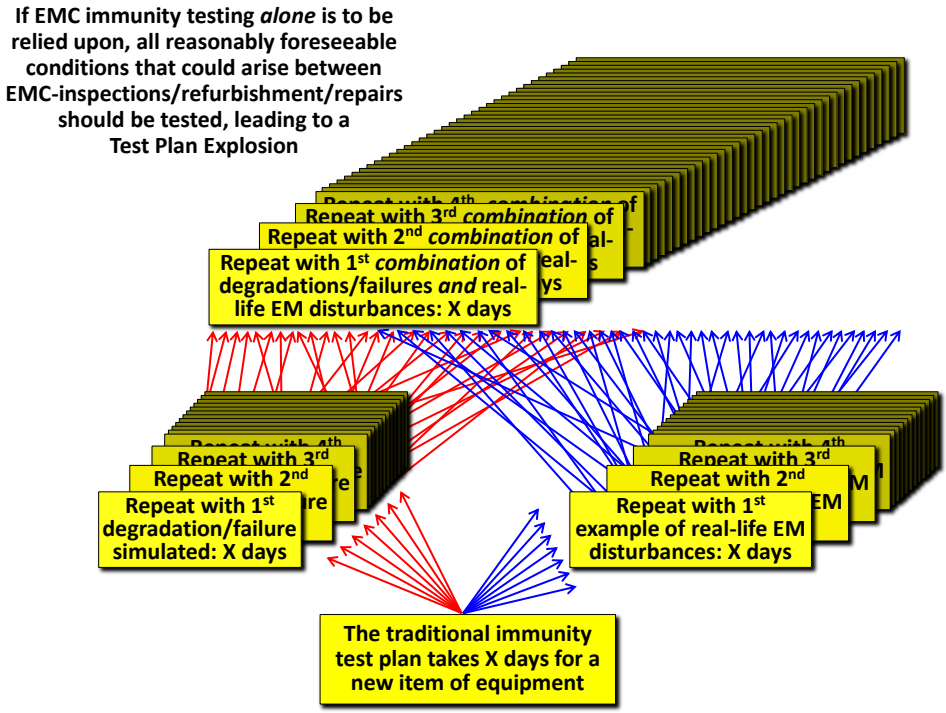
c) Foreseeable combinations of a) plus foreseeable combinations of b), during the lifecycle, for example:

- Two or more radiated fields at different frequencies
- A radiated field at any frequency plus an Electrostatic Discharge (ESD) event at any location and 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.

Michel Mardiguian showed in [13] that when one EM disturbance is applied (e.g. a radiated RF field) the immunity of the equipment to another disturbance (e.g. fast transient bursts) can be seriously compromised. In his conclusions he stated:

"Speculating that all the worst EMI threats will appear at the same time on a given system would be extravagant. But relying on the belief that certain EMI combinations will never exist could be just as imprudent."

It very quickly becomes obvious that trying to cover all these reasonably foreseeable situations over the lifetime would create a "test plan explosion", as shown below.



Even if only 50 sets of tests were sufficient to simulate a), b) and c) respectively, this would require the immunity tests to be repeated 150 times. Few could afford to wait that long!

So, what are we to do about the functional safety risks that can be caused by EMI?

IET Standards published a Code of Practice on what it calls "Electromagnetic Resilience" in 2017 [14], and IEEE Standards is developing this further [3]. In the next article, "Management of Functional Safety Risks caused by Electromagnetic Interference" we provide further details of these publications and describe some current best practice techniques in managing EMI System Safety risks.

References

[1] K. Armstrong, "Why EMC Immunity Testing is Inadequate for Functional Safety," IEEE 2004 Int. Symp. EMC, Santa Clara, CA, August 9-13, ISBN: 0-7803-8443-1

[2] K. Armstrong, "Why increasing immunity test levels is not sufficient for high-reliability and critical equipment" IEEE 2009 Int. Symp. EMC, Austin, TX, Aug. 17-21, ISBN: 978-1-4244-4285-0

[3] IEEE Standards Association, project P1848, "Techniques and Measures to Manage Functional Safety

and Other Risks with Regard to Electromagnetic Disturbances", standards.ieee.org

[4] "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." from: "The Quality Attitude", Watts S. Humphrey, Carnegie Mellon University, November, 2009, on page 131 of resources.sei.cmu.edu/asset_files/SpecialReport/2009_003_001_15035.pdf.

[5] "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." An extract from: "A New Accident Model for Engineering Safer Systems," Professor Nancy Leveson, Massachusetts Institute of Technology (MIT), USA, "Safety Science," Vol. 42, No. 4, April 2004, pp. 237-270: sunnyday.mit.edu/accidents/safetyscience-single.pdf

[6] "We have looked at what it takes to validate autonomous driving, and the time needed was estimated at 100,000 years." Michael Bolle, in "Car safety and the digital dashboard" Chris Edwards, E&T Mag., 13 Oct. 2014, eandt.theiet.org/content/articles/2014/10/car-safety-and-the-digital-dashboard/

[7] "Building Robust Systems, an essay", G. J. Sussman, MIT, Feb. 23, 2008, groups.csail.mit.edu/mac/users/gjs/6.945/readings/robust-systems.pdf

[8] "Computer systems lack 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." from "Computer Based Safety-Critical Systems," The IET, September 2008 (this quotation does not appear in the 2013 edition)

[9] J. A. Whittaker, "What Is Software Testing and Why is it so Hard", IEEE Software, Jan-Feb 2000, pp 70-79 ieeexplore.ieee.org/document/819971

[10] "New DRIVE PX 2 Uses Deep Learning and Supercomputing to Enable Cars to Sense Surroundings, Navigate Autonomously", Jan 4, 2016, nvidianews.nvidia.com/news/nvidia-boosts-iq-of-self-driving-cars-with-world-s-first-in-car-artificial-intelligence-supercomputer

[11] D. Evans, "The Internet of Things. How the Next Evolution of the Internet Is Changing Everything", April 2011, www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[12] F Beck and J Sroka, "EMC Performance of Drive Application Under Real Load Condition", Schaffner EMV AG Application Note, 11th March 1999.

[13] M. Mardiguian, "Combined effects of several, simultaneous, EMI couplings", M. Mardiguian, 2000 IEEE Int. Symp. EMC, Washington D.C., ISBN 0-7803-5680-2, pp. 181-184.

[14] "Code of Practice on Electromagnetic Resilience", The IET, 2017, www.theiet.org/resources/standards/emr-cop.cfm

Keith Armstrong C.Eng, FIET, Senior MIEEE Cherry Clough Consultants Ltd, UK.

Keith graduated from Imperial College, London in 1972 with an Honours Degree in Electrical Engineering. He is a Fellow IET and Senior Member of IEEE, has chaired the IEE/IET Working Group on EMC and Functional Safety since 1997, and is UK's appointed expert to several IEC EMC standards committees.

Prof. Davy Pissoort, Senior MIEEE, Boydens Mechatronics Group.

Davy received his PhD degree in electrical engineering from Ghent University, Belgium in 2005 and worked as an R&D Engineer at Agilent Technologies (now Keysight Technologies) in Ghent. For the last 10 years he has been an associate professor and head of the Mechatronics Group at KU Leuven Bruges Campus.