Why is the IEEE Developing a Standard on Managing Risks Due to EM Disturbances?

Prof. dr. ir. Davy Pissoort
Research Group ReMI - Reliability in Mechatronics & ICT
KU Leuven, Technology Campus Ostend, Belgium
davy.pissoort@kuleuven.be

Keith Armstrong
Cherry Clough Consultants Ltd, U.K.
keith.armstrong@cherryclough.com

Abstract

The IEEE Standards Association is developing a standard to deal with the problem of managing risks that can be caused by electromagnetic (EM) disturbances, which will not rely solely on immunity testing, making it a new type of EMC standard.

Where failures in electronic equipment can cause Functional Safety or other risks to be higher than considered acceptable at any time during its lifecycle, the proportion of those failures that could be caused by electromagnetic (EM) disturbances must be taken into account as part of the Risk Management process.

However, immunity testing alone is incapable of providing sufficient design confidence, however much the test levels are increased, and this paper describes why and the reasons for this new IEEE standard.

Keywords—Electromagnetic Compatibility; Electromagnetic Interference; Functional Safety; Electromagnetic Security, Risk Management.

I. Introduction

Most of the EMC testing industry worldwide appears to believe that EMC testing covers everything that is needed regarding protection from EM disturbances, and – if there are Functional Safety or other risk management issues – all that is required is to increase the levels on the immunity tests by enough to create a (so-called) "Safety Margin".

The author debunked this myth at the IEEE EMC Symposium in 2004 [1] and again in [2], but it is still a widespread myth so – with the work on the new IEEE Standard on "*Techniques and Measures to Manage Risks with Regard to Electromagnetic Disturbances*" [3] getting underway this year it seems timely to revisit the reasons why no amount of immunity testing, whatever the test levels used, can demonstrate that a digital device or system can have low-enough risks from EM disturbances to be used in Functional Safety or other risk-managed applications.

II. Determining 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 1 ppm/person/year.

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

Some of the most dangerous occupations have been estimated by the HSE to have risks of death around 1000 ppm/person/year, and following the usual method a risk target of 100 ppm/person/year would be allocated, due to EM disturbances alone, a design confidence of 99.99%.

This level of confidence should be compared with the confidence in knowing what the real-world EM environment of any given system will be, over its entire lifecycle.

The normal EMC immunity test standards, for example as listed under the European Union's EMC Directive, are claimed to cover 80-95% (depending on the 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 required 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 are excluded although they would certainly be expected to occur during any typical lifecycle.

(The author fails to understand why these test standards still do not cover the very close proximity (e.g. closer than 25 mm) of cellphones and other personal electronic devices containing low-power radio transmitters, even though this has become a commonplace situation and with the Internet of Things (IoT) will soon become ubiquitous.)

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 99.99% of a specified EM environment for a year or more.

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

- Roll-out of 5G cellphone systems with 100-times the data bandwidth of current benchmarks is expected to be well-underway by 2020, but its frequency ranges, modulation types 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 which will in turn increase their use in many more applications, including all domestic appliances. Unfortunately, switching faster will also make them noisier, at much higher frequencies.
- Switching power converters will increasingly be connected to the AC power grid due to the increasing take-up of alternative energy generation (e.g. photovoltaic), both small and large-scale, making the power grid noisier.
- LED lighting will replace most incandescent and fluorescent lighting, using switch-mode power conversion that is much noisier than those technologies.
- Wireless Power Transfer (WPT) will use switching power converters to generate magnetic fields to couple with remote devices with sizes up to and including automobiles, trucks, buses and trams. Up to 50% of these noisy fields will not couple with their target devices and will "leak" into the environment. Close proximity to WPT chargers will expose devices to intense disturbances, and it would be very difficult indeed to ensure that this cannot happen.
- The use of PowerLine Telecommunications (e.g. 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 Readers.
- Machine-to-Machine (M2M) wireless datacomunications is expected to increase dramatically due to so-called Industry 4.0 and the IoT.
- Automobile safety systems will increasingly use steered radar beams of a few watts at frequencies including 76GHz, and modern silicon devices at 28nm or less are becoming increasingly susceptible to such frequencies.
- 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 rectifiers and switching power converters.
- 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.
- Experts estimate that the IoT will consist of almost 50 billion objects by 2020 [4], and most of these will communicate using wireless datacommunications.

It is clear that it is impossible to know, with any suitable degree of confidence, what types of EM disturbances should be tested, and the test levels to use, to be capable of demonstrating that EM disturbances cannot cause unacceptable levels of risk during a lifecycle. Figure 1 attempts to show this problem graphically.

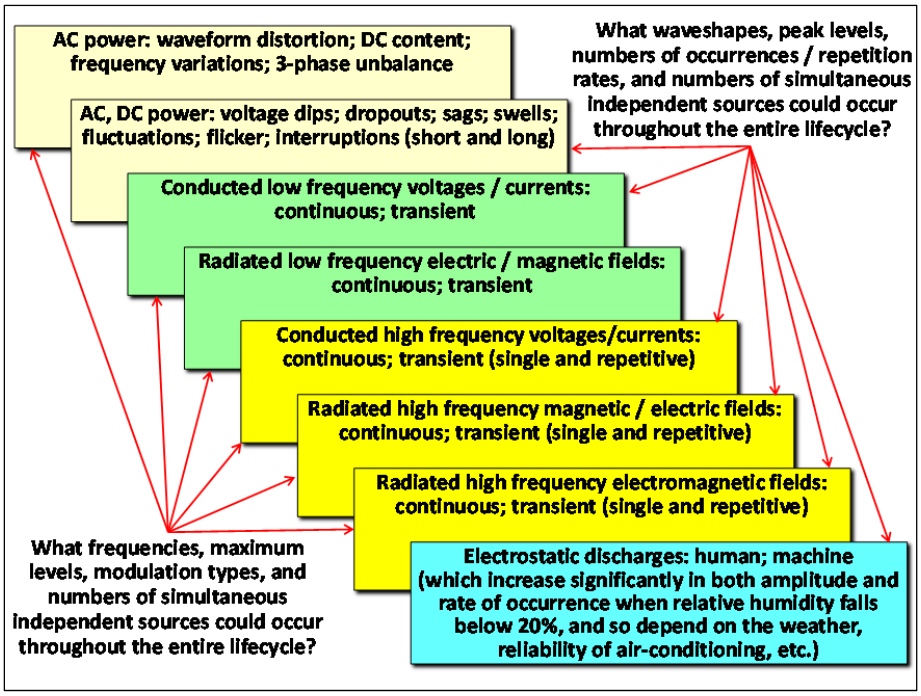

Figure 1 The problem of predicting the future EM environment with sufficient accuracy for managing risks measured in ppm/year

III. 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 and its software could get into, see [5] [6] and [7]. The author understands that the state of the art in 2013 was that Microsoft could fully test all the states of a 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, testing a percentage of possible states makes it possible to predict the behaviors of the untested ones. Unfortunately, all digital systems are *non-linear*, which means that even if it was possible to test 99% of all their possible states, the test results could not be extrapolated to provide any reliable information about the behavior of the remaining 1%, see [8].

This results in a well-known problem: digital systems can fail in an unpredictable manner as the direct result of untested combinations of *perfectly correct inputs*, [9]. For example, if a digital system had four inputs each digitized to 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, about $2 \cdot 10^{12}$. 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 system states than are required for just the "input space", not least to handle the processing of the input data, and to discover whether EMI could cause an unsafe error or malfunction by immunity testing alone would require each EMC test to be applied 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) 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. For the simple example system above, this would take 2.3 days. Then the test frequency would be stepped 1% higher for another 2.3 days, and 230 such steps would cover one decade of frequency, taking nearly 1.5 years, 24/7. The whole process would then be repeated with three other angles of incidence, and again with 90° antenna polarization.

So even the simple example system discussed earlier would need 12 years of EMC testing (24/7) to perform an IEC 61000-4-3 test covering just one frequency decade, on its "input space" alone.

Assuming all of the digital states (not just input space) could be tested in 5 days, and testing 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 four test levels of ESD on 10 test points would need about 58 years of testing, 24/7.

Of course, this is all a gross simplification: clever testing techniques might be able to be used to reduce the testing time; and it might also be possible to speed up the testing of the system states. Assume that "intelligent" digital testing techniques reduce the number of states to be tested by 10 (without, of course, compromising our design confidence of between 99.99% and 99.99999%); this simple example of a safety-related system could be EMC tested in about 6 years. Although most EMC test laboratories would be very pleased to provide this amount of testing, even if their customers could afford the cost almost no-one could countenance such a long delay in their project.

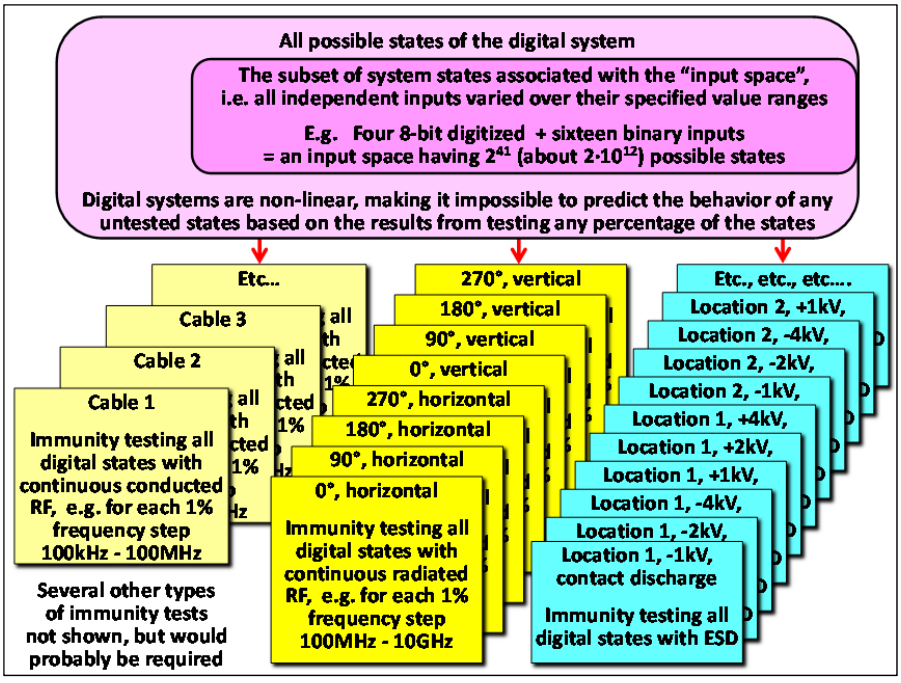

Figure 2 The problem of testing a sufficient number of digital states to manage risks which are measured in ppm/year

The above example is possibly unrepresentative of future mass-produced safety-related systems, such as the DRIVE PX 2 described in [10]. Assuming this to have eighteen 8-bit digitized monochrome camera inputs, 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 just 10 nanoseconds per test, 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).

The author accepts that these are *very* crude worked examples, but nevertheless the huge difference between what would normally be considered a large but acceptable immunity test schedule for a safety-related system and the time required to perform basic immunity tests on the input space only, is more than enough to 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. Figure 2 attempts to show this problem in a sketch.

IV. The Exploding EMC Test Plan

Assuming that a design confidence of between 99.99% and 99.99999% is required as regards risks caused by EM disturbances over the entire lifecycle of a system, and assuming for the sake of argument that the problems discussed above have somehow been dealt with, the suite of immunity tests would have to be performed many times to simulate the following real-life situations:

a) Reasonably foreseeable degradations and failures in each EMC-significant component or connection (e.g. connector pins, solder joints, filter ground connections, etc.), throughout the entire lifecycle. These could be caused, for example, by: initial tolerances; aging; corrosion; use and 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 a) *plus* foreseeable combinations of b), during the 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 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.

It very quickly becomes obvious that trying to cover all these reasonably foreseeable situations over the lifetime would create a "test plan explosion", as Figure 3 attempts to show. Even if a digital system could possibly be immunity tested to the appropriate level of design confidence in a reasonable time, and even if only 50 sets of tests could simulate a) above; 50 sets cover b), and 50 sets cover c), this would require the immunity tests to be repeated 150 times. And if, somehow, the cost was considered affordable, few could afford to wait that long!

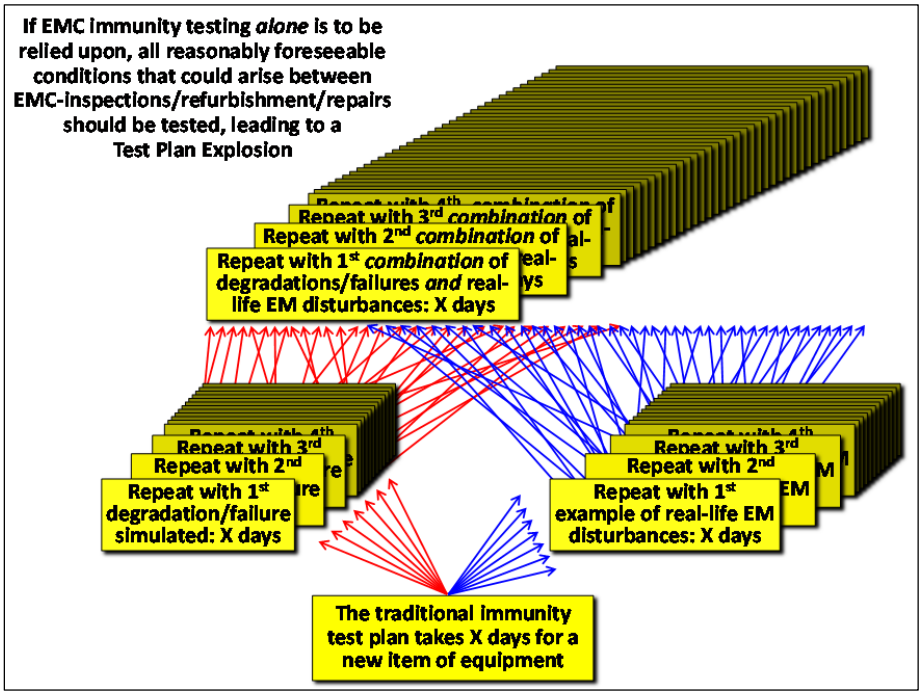

Figure 3 The problem of the exploding test plan

Michel Mardiguian showed in [11] 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. Crude modeling, and a series of three simple tests are suggesting that within the frame of what has been simulated, the combination of effects is a real risk. ….for those applications where combined threats could happen, the product specification or the test plan should require a greater EMC margin, to cover a possible simultaneous exposure."*

V. EMC test Standards Do Not Simulate Real EM Environments Well Enough

EMC test methods are designed for accuracy, repeatability, and low cost – and may not simulate real life very well. For example: most radiated EM field immunity testing is done in anechoic chambers that create an environment unlike every 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 5kHz, whereas the EM disturbances from the electro-mechanical contacts that the EFT/B test is intended to represent actually varies in frequency from MHz to kHz as the contact gap opens, with a rising amplitude as frequency decreases.

Another example: electronic warfare and munitions 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. The author has been involved with two situations where equipment passed tests with any 1 kHz sine-wave modulated frequency at 100 V/m, but were at least 80 dB more susceptible (i.e. to 10 millivolts/m) when the modulation frequency was set to a circuit's operating frequency. Both of these situations were discovered by accident because they were required to be tested with 1 kHz square-wave (pulse modulation) and their especially-susceptible frequencies happened to lie very close to one of its harmonics. Both used AC-energized sensors, and both would cause severe financial and/or safety problems if interfered with in normal operation.

[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. EMC testing standards usually test at just one setting of the equipment's load – but it is well known that the levels of current flowing in the inductors of a filter will alter their inductance values due to variations in permeability (and even saturation). EMC testing standards also test at just the nominal value of the mains voltage – whereas higher or lower voltages will alter the currents in the supply filters' inductors and thereby alter their inductance values. Also, EMC testing standards only test at one ambient temperature – but it is well known that inductance varies with temperature.

These variations will alter the characteristics of power filters, affecting the emissions and immunity of the equipment. [13] gives the example of a variable-speed motor drive tested for emissions to IEC 61800-3, at 25°C and 230Vrms with a light load on the motor. When retested at 40°C, +10% supply voltage, and full load, the emissions from the variable speed drive were measured to be 20dB higher, indicating that the equipment's supply filter's performance had fallen by 20dB.

VI. What Should Be Done to Deal With All these Testing Problems?

The military have traditionally dealt with the above four 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 approach, the author calls it the "Big Grey Box" (BGB) method. Unfortunately, the BGB method 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 "IEC Basic Safety Publication" [14] 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.

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

EMI actually means errors, malfunctions or failures 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 on "Techniques and Measures to Manage Risks with Regard to Electromagnetic Disturbances" [3] 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 [15], to ensure that acceptable safety risk levels will not be exceeded by any reasonably foreseeable EMI over the lifecycle.

This alternative, practical approach to the BGB was first described in [16], and effectively means that any EMI which occurs because of EM disturbances outside the tested parameters, or because of any of the other problems discussed above, is detected by the system itself. If the effects of the EMI could increase safety risks above acceptable levels, they are either corrected, or the system is switched into one of its safe states, or switched to an unaffected back-up system. For more details, see [17].

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.

References

[1] "*Why EMC Immunity Testing is Inadequate for Functional Safety*," Keith Armstrong, IEEE 2004 Int. Symp. EMC, Santa Clara, CA, August 9-13, ISBN: 0-7803-8444-X

[2] "*Why increasing immunity test levels is not sufficient for high-reliability and critical equipment*" Keith Armstrong, IEEE 2009 International Symposium on EMC, Austin, TX, August 17-21, ISBN: 978-1-4244-4285-0

[3] IEEE Standards Association, project P1848, "Techniques and Measures to Manage Risks with Regard to Electromagnetic Disturbances", http://standards.ieee.org/

[4] "*The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*", Dave Evans, www.iotsworld congress.com/documents/4643185/0/IoT_IBSG_0411FINAL +Cisco.pdf; https://en.wikipedia.org/wiki/Internet_of_Things

[5] "*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*." An extract from: "*The Quality Attitude*,"Watts S. Humphrey, Carnegie Mellon University, March 1, 2004, www.sei.cmu.edu/library/abstracts/news-at-sei/ wattsnew20043.cfm

[6] "*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: http://sunnyday.mit.edu/accidents/safetyscience-single.pdf

[7] "*With autonomous driving new questions arise. To do automated braking you need a certain amount of validation. We have looked at what it takes to validate autonomous driving, and the time needed was estimated at 100,000 years.*" Michael Bolle quoted in "*Car safety and the digital dashboard*", Chris Edwards, E&T magazine, vol. 9, iss. 10, 13 Oct. 2014, http://eandt.theiet.org/magazine/2014/10/car-safety.cfm

[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, Sept. 2008: www.theiet.org/factfiles/it/computer-based-scs.cfm?type=pdf

[9] "Robustness (computer science)", https:// en.wikipedia.org/wiki/Robustness_(computer_science)

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

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

[13] IEC 61508 "*Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*" in seven parts, available from https://webstore.iec.ch

[14] "*Basic Safety Publications*", The IEC, www.iec.ch/about/ brochures/pdf/tools/BasicSafetyPublications_2011.pdf

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

[14] "*Basic Safety Publications*", The IEC, www.iec.ch/about/ brochures/pdf/tools/BasicSafetyPublications_2011.pdf

[15] "*Non-Standardized Immunity Test Techniques to Help Manage Risks caused by EM Disturbances*", Davy Pissoort and Keith Armstrong, IEEE 2016 International Symposium on EMC, Ottawa, Canada, July 2016

[16] "*Overview of techniques and measures related to EMC for Functional Safety*," The IET, London, U.K., August 2013, www.theiet.org/factfiles/emc/emc-overview.cfm

[17] "*How to Manage Risks with Regard to Electromagnetic Disturbances"*, D. Pissoort and K. Armstrong, IEEE 2016 Int. Symp. EMC, Ottawa, Canada, July 2016