emc STANDARDS

Another EMC resource
from EMC Standards

Developing Immunity Testing to Cover Intermodulation

Helping you solve your EMC problems

Developing Immunity Testing to Cover Intermodulation

Dipl. Ing. (FH) Werner Grommes
Niederkassel, Germany
gr@unitybox.de

Keith Armstrong, IEEE Senior Member
Cherry Clough Consultants Ltd, UK
keith.armstrong@cherryclough.com

***Abstract* – Existing immunity test methods can be developed to cost-effectively provide greater "coverage" of real-world electromagnetic environments, and such techniques are now needed to aid effective risk management of electromagnetic compatibility (EMC) because of the increasing automation of society and industry.**

The reliability of electronic technologies (including their software and firmware) becomes critical when the consequences of errors, malfunctions or other types of failure include significant financial loss, mission loss, loss of security, or harm to people, domestic animals or property (known as "functional safety").

Electromagnetic interference (EMI) can be a cause of unreliability in all electronic technologies, so EMC must be taken into account when the risks caused by malfunctioning electronics need to be controlled.

Unfortunately, it is not practicable to achieve the levels of confidence required for critical systems, over their entire lifetime, by EMC testing alone – no matter by how much the test level is increased above the maximum levels obtaining in the environment. A variety of *additional* verification and validation techniques are required.

The subject of this paper is developing existing radiated and conducted radio-frequency immunity test methods to cover real-life possibilities for intermodulation, that at the time of writing are ignored by almost all standardized test methods.

***Keywords* – Cost-effectiveness, EMC, EMI, functional safety, high-reliability, mission-critical, reliability, risk analysis, safety-critical, security, safety risks.**

I. INTRODUCTION

Professor Shuichi Nitta says, in [1]: "*The development of EMC Technology taking account of systems safety is demanded to make social life stable.*" The authors hope that this paper makes a useful contribution to this work.

Electronic devices and circuits of all types, and the software or firmware that runs on them, are susceptible to errors, malfunctions and other types of failure caused by electromagnetic interference (EMI) from the electromagnetic (EM) disturbances they are exposed to during their lifetimes [2].

"High reliability", "mission-critical", "safety-critical" or security applications might need to have a meantime to failure (MTTF) of up to 100,000 years (corresponding to Safety Integrity Level 4 (SIL4) in [3], see Figures 1 and 2 in [4]), possibly even more.

Mass-produced products (e.g. automobiles, domestic appliances, etc.) could also require very low levels of safety risk, because of the very large numbers of people using them at any given time.

EMI has long been recognized as a cause of unreliability in electronic equipment, especially by the military and aerospace industries, and as a result EM immunity test methods and regimes have been developed.

Existing immunity tests have generally been successful in reducing the failure rate due to EMI for financial reasons (e.g. controlling warranty costs). As electronic technology continues to advance, these immunity tests also advance to keep pace.

But any EMC testing regime that has an affordable cost and duration is very unlikely to be able to demonstrate confidence in achieving reliable-enough operation, even for applications with quite low criticality [4] [5] [6] [7].

The solution is to use well-proven EMC design techniques to reduce risks, verifying and validating them using a number of different methods, including (but not limited to) immunity testing.

None of these methods is complete in itself, and they can each be regarded as providing a different perspective on the design in question. It is as if each technique was a spotlight that illuminated certain aspects of a design very well indeed, but left much of the design in shadow. By shining a number of spotlights from many different angles, we highlight many more design aspects, increasing our confidence that we know as much as we need to for ensuring risks are as low as required.

Given sufficient levels of detailed analysis, from enough different perspectives, we can be confident that we have covered all that is necessary to achieve a safe-enough design.

The *general* subject of this paper is developing existing EMC immunity test methods to extend their coverage of the real-world EM environment. In terms of the above analogy, we might describe this as widening the width of a source of illumination, so that it reveals more of a design.

The *specific* topic of this paper is extending or developing the existing continuous radio-frequency (RF) immunity test methodologies to cover the simultaneous presence of two or more frequencies, at significant levels, in the real-world EM environment, so that they cover intermodulation possibilities.

Part II of this paper discusses some of the ways in which simultaneous frequencies, at significant levels, can arise in a real-life electromagnetic environment (EME), and how cur-

Presented by Keith Armstrong at the IEEE 2011 Int'l Symposium on EMC, Long Beach, California, August 15-19, ISBN: 978-1-45770810-7

rent single-carrier-frequency immunity test methods fail to address their intermodulation effects.

Part III describes the authors' current proposals for developing the existing test methods to cover intermodulation from any number of simultaneous frequencies.

II. Simultaneous Frequencies in the Real EME

Two or more radio channels are often present in an environment, at significant levels, and the following are some examples.

It is not unusual to be near two or more cellphones on which calls are being made. In a typical waiting area for a train or airplane, or in a train carriage, having two or more cellphone calls being made within a few meters is almost the normal situation.

Where there are two or more first-responder vehicles present (e.g. police and ambulance, ambulance and fire engine) or two or more taxicabs or delivery trucks, multiple radio fields will often be present at significant levels up to tens of meters away.

If there is a single significant field over an area, for example from a broadcast transmitter, taxi or delivery dispatcher office, first-responder vehicle, taxicab, delivery truck or amateur radio operator, use of a cellphone makes it a multiple-frequency environment.

Broadcast transmitting stations and base-stations generally transmit at multiple frequencies simultaneously.

Wi-Fi, Bluetooth and similar devices operating the ISM bands fill them with multiple frequencies, even to the extent that in some environments it can be hard to find available channels.

Airfields, harbors and the like operate scanning radars, VHF and UHF communications simultaneously.

Some vehicles are equipped with multiple radio transmitters, especially large ships (both civilian and military).

As electronic device technology develops, and as the spectrum regulations change, the RF spectrum is becoming more crowded, to the extent that an important current development project is "software radio" – radiocommunications that can use any available frequencies over a wide frequency range – to take advantage of gaps in the spectrum that might open up only temporarily.

Power Line Communication (PLC) sometimes called PLT or BPL (Broadband Over Powerline) technologies emit high levels of noise into the mains power distribution network over a wide range of frequencies simultaneously, for example from 2MHz to 26.5MHz [8], generally with some "notches" for the common short-wave radiocommunication bands.

Figure 1 shows the effect of two frequencies, chosen as 400 and 500MHz for easy calculation, on an electronic circuit.

It shows that these two frequencies are rectified by the non-linearities in the semiconductors to generate baseband noise (the sum of the demodulated envelopes) plus harmonics of the original signals. Only the second-order harmonics of the two example frequencies will fit within the scale of Figure 1, but of course there are also thirds, fourths, fifths, etc.

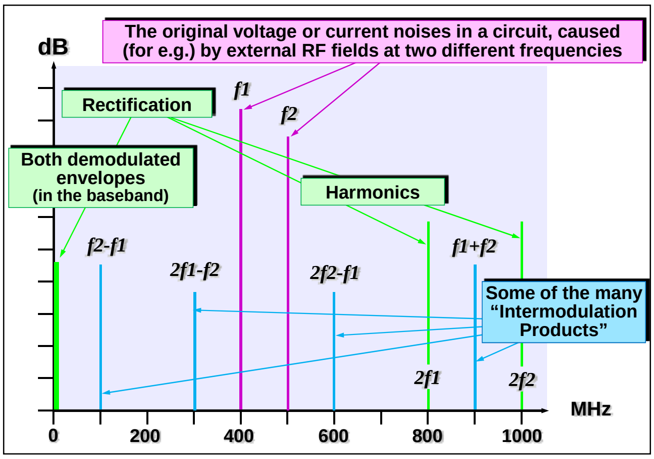

Figure 1 Demodulation and intermodulation

The semiconductor (and other) non-linearities also cause mixing of the signals, so we get the sum and differences of the two initial signals, in this case at 100MHz and 900MHz. These are known as "1st order IM products", and there are just two of them.

Then the 2nd order harmonics intermodulate with each other, and with the original signals and their sum and difference frequencies, giving $2f2 - f1$, $2f2 + f1$, $2f1 - f2$ $2f1 + f2$, $2f2 - 2f1$ and $2f2 + 2f1$. These are known as "2nd order IM products", and there are six of them. Only a few of them appear within in the frequency scale chosen for Figure 1. In general, 2nd order IM products are lower in level than 1st order products.

Next, the 3rd order harmonics interact with the 2nd order harmonics and with the original signals plus their sum and difference, giving a large number of 3rd order IM products, generally at a lower level than the 2nd order. And so on with the 4th, 5th, 6th etc., IM products.

Figure 1 only shows IM products up to the 2nd order, but in reality the two signals at 400 and 500MHz would create dozens of IM products in the frequency range up to 1GHz.

Because the example frequencies were simple numbers, many of their IM products will fall on the same frequencies, but this would not generally be the case for real-life intermodulation events.

Now, imagine we are in a regular EMC test laboratory, performing RF immunity tests, which all use a single carrier frequency (and usually a simple amplitude modulation, such as a 1kHz sinewave).

When tested with a single frequency over 10kHz to 10GHz, we might find that equipment under test (EUT) is susceptible over the range 10kHz to 100MHz.

Being good EMC engineers, we add filtering and shielding that is effective over the range 10kHz to 100MHz, so that the EUT passes the test. The mitigation we use is ineffective above 500MHz, and might even resonate at higher frequencies, but we are under pressure not to increase manufacturing costs by any more than is essential, so we do the minimum required to pass the test.

We pat ourselves on the back for doing a good job, and move on to the next EUT to be tested and made to pass.

But when the EUT is used in a real-life EME that has two or more frequencies present at significant levels above 500MHz, they are not prevented from entering the EUT's circuits and their intermodulation can easily create internal noise in the 10kHz to 100MHz band – causing interference.

Single-frequency testing at any level will not find this real-life susceptibility [9].

It is commonplace to hear people saying that the standard RF immunity tests provide immunity against real-life EMEs, but it is easy to see that this is impossible, making it impossible to use the standard RF immunity tests to "prove" that an equipment or system has adequate reliability to control safety risks in real life applications.

This discussion begs the question about what levels of RF are "significant". This will of course depend on the particular design and realization of the devices and circuits in the EUT in question, and the level of safety (or other) risk that is considered to be acceptable.

The highest sensitivity that one of the authors has seen, was a gas flow meter that measured the Doppler shift in ultrasound beams caused by the speed of gas flow through a specified cross-sectional area. When tested with RF modulated by 1kHz sinewave, it suffered no interference at up to the limit of the test lab used – 100 V/m. But when the test signal generator was switched to squarewave (as required by the relevant gas industry standards) it failed at 1V/m.

It turned out that the EUT could only withstand a 5 *millivolts*/meter field at the frequency used by its ultrasound beams. This frequency just happened to be exactly the 171st harmonic of 1kHz, and if it had not been the square-wave test would probably have been passed at the required level of 30V/m.

This example shows that some circuit designs can be very susceptible indeed at certain frequencies, whether these result from carrier-waves, demodulated envelopes, or intermodulation. In this case, the EUT was about 85dB more sensitive to a certain modulation frequency than it was to the normal 1kHz sine modulation used in the tests.

Intermodulation resulting in an IM product that coincides with such a very susceptible frequency is a real possibility, which means that interference could be caused by a rather exotic IM product, such as $29f2 - 18f1$, that would be expected to arise in the semiconductors but at a very low level.

Considering frequencies in the ultrasound range from 100kHz to 1MHz, we have the possibilities of carrier-waves from radio transmissions and the emissions from variable-speed motor drives (and other powerful switch-mode converters) at their switching frequencies and first hundred harmonics.

Digital modulation techniques include some with frequencies in that range, possibly causing interference by baseband demodulation. And IM products that lie in this frequency range are of course possible over the full range of frequencies that the semiconductors themselves will respond to – at least 5GHz at the time of writing.

The reliability of equipment and systems that are especially susceptible at particular frequencies therefore depends upon the likelihood that those frequencies will arise in their operational EMEs, either directly, or as modulation or by intermodulation.

Some people would say that most equipment functions perfectly reliably in its real-life EME, providing it passes the appropriate immunity tests that are used at the moment, for example IEC 61000-4-3 and 61000-4-6. But how much is "most"?

The committees that created 61000-4-3 and 61000-4-6 say that they aimed for a "technical/economic compromise" of 80% confidence, and that they specifically did *not* consider safety-related or high-reliability applications.

But 80% is significantly lower than the minimum confidence level of 90% required for the lowest level of safety integrity ("SIL1") for any safety-related system by the IEC's basic standard on Functional Safety, IEC 61508 [3].

SILs in [3] go up in decade steps to SIL4, which is the level considered necessary for railway signaling systems and safety systems in nuclear power plant, which requires a confidence of between 99.99% and 99.999% for every 10,000 hours of continuous operation, equivalent to a mean-time-to-dangerous-failure range from 10^8 to 10^9 hours (i.e. approximately 11,400 to 114,000 years).

Nobody can possibly claim to have the *direct* experience that shows that their "most" encompasses the levels of reliability of SIL 2 (99% to 99.9%) or higher, for every kind of electronic equipment or system that will ever be built.

And claims of *indirect* experience are always suspect because operator error is so commonplace that electronic errors and malfunctions caused by interference – that generally leave no trace of their cause – are usually attributed to operator error.

Also, accident investigators are rarely EMC specialists, so EMI possibilities are usually not investigated correctly – where they are investigated at all.

Since our engineering analysis shows that multiple RF sources can cause IM products that can in turn cause interference in many types of circuits, for safety and high-reliability engineering we have to deal with this.

In most applications, it is effectively impossible to determining the likelihood that two or more frequencies could cause an IM product that coincided with an especially susceptible frequency.

The only safe course of action is to assume that if it can happen, it will, at some time. (And it does happen. [10] includes several anecdotes of EMI caused by intermodulation in real life.)

One method of dealing with the problem of intermodulation is by design and design assessment. For example, if the equipment or system was completely enclosed in high-specification shielded cabinets; was powered from internal batteries or motor-generator sets that guaranteed "clean" power, and used only fiber-optics for signal and data communications – then, subject to an assessment of the assembly details and workmanship quality – it could easily be possible to declare that it would be perfectly resistant to its EME without performing any immunity tests on the finished item.

But, in practice, not every type of equipment can be enclosed in large, heavy (costly) gray metal boxes with such costly mitigation for the RF noises on their power and signals.

So we need to develop test methods – if we can – that provide better coverage of the multiple frequencies that can exist in real-life EMEs – the subject of the next Part of this paper.

III. A Proposal For Developing RF Immunity Tests

This proposal is based on the existing continuous RF immunity test method IEC 61000-4-3 (radiated) and -4-6 (conducted), to provide very much greater test "coverage" for the reasons outlined in Part II.

It is very similar indeed to the antenna intermodulation and "cross-modulation" test methods CS103 and CS105 in MIL STD 461F [11].

At the time of writing it is just an unproven idea, although it would be easy to try out, and the authors hope to do this during 2011. There seems to be no reason why this new method should increase test times.

Two (or more) frequencies *f1* and *f2* are combined electronically, amplified, and – for radiated tests – input into one antenna that illuminates the EUT in a test set-up that otherwise follows IEC 61000-4-3 exactly.

f1 is swept as per 61000-4-3, with *f2* initially set to twice the *f1* start frequency. When *f1* reaches *f2*, *f2 is* doubled, and this process is repeated up to the maximum value of *f1*.

For example, if *f1* is to cover 80MHz to 3GHz, set *f2* initially to 160MHz, then 320, 640, 1280, 2560 and finally 3000MHz.

The use of this "twin-tone" RF test signal will generate IM products in semiconductors and other non-linearities in EUTs, causing a comb of frequencies rather than the simple single carrier-wave plus 1kHz sinewave baseband noise created by the standard tests.

Figure 2 shows the schematic used for some simulations of the probable effect of this sort of test applied to a diode (D1) using a resistive summing circuit.

The lower graph in Figure 3 shows the spectrum of the voltage at the summing resistor, R4, with two RF signals at 850 and 875MHz, from 10MHz to 10GHz.

It shows the 1st order IM products in the diode at 25MHz and 1.725GHz, plus the 2nd and higher-order IM products in the diode as signals with 25MHz spacings either side of the source frequencies.

The diode voltage appears at R4 because the 1kΩ resistor in series with the diode does not provide perfect isolation, and the simulation has a very large dynamic range (200dB).

The upper graph in Figure 3 zooms the frequency range in, to take a closer look at the 2nd and higher-order IM products.

Figure 4 shows the simulation of the diode D1 voltage, showing that the 1st order IM products are about 10dB below the level of the two sourced frequencies, the 2nd order IM products are at about -22dB, 3rd order at -30dB, 4th at -37dB, etc.

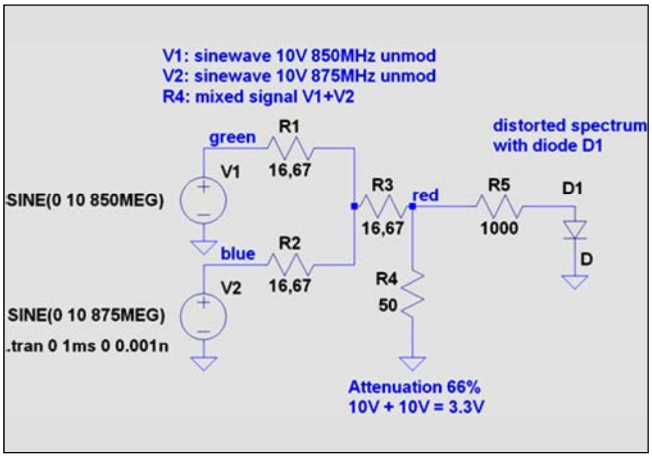

Figure 2 The simulated circuit

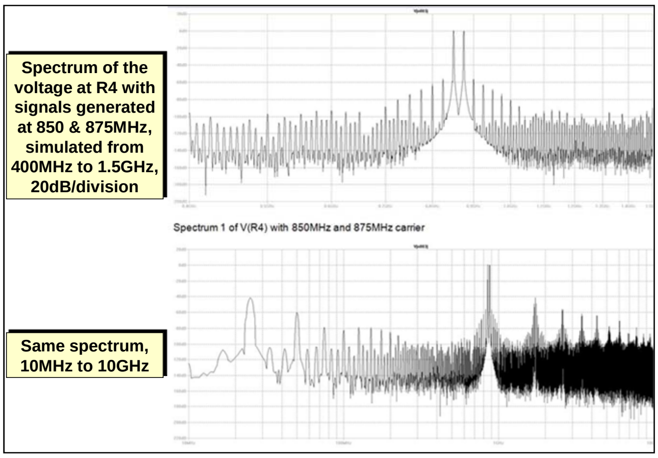

Figure 3 Simulated voltages at R4 in Figure 2

So we can see that exposing EUTs to two or more simultaneous frequencies will generate IM products in its semiconductors (not that this was ever in doubt).

Alistair Duffy and Antonio Orlandi have demonstrated a reverberation chamber test method that shows promise for testing radiated field immunity with more than one simultaneous RF frequency to test intermodulation effects [12] [13].

Using the very simple twin-tone test described above does not increase test time, although it adds to the cost of test instrumentation in four ways:

- Generating an additional programmable frequency (not relevant if an arbitrary signal generator is used)
- Summing the two source signals (not relevant if an arbitrary signal generator is used)

Presented by Keith Armstrong at the IEEE 2011 Int'l Symposium on EMC, Long Beach, California, August 15-19, ISBN: 978-1-45770810-7

- Doubling the RF power amplifier rating so that it can source both signals to the antenna at the maximum level in the test method with insignificant distortion (some RF PAs may have enough headroom already)
- Increasing the RF power rating of the antenna, to be able to emit both signals into the chamber with insignificant distortion (some antennas may have enough headroom already)

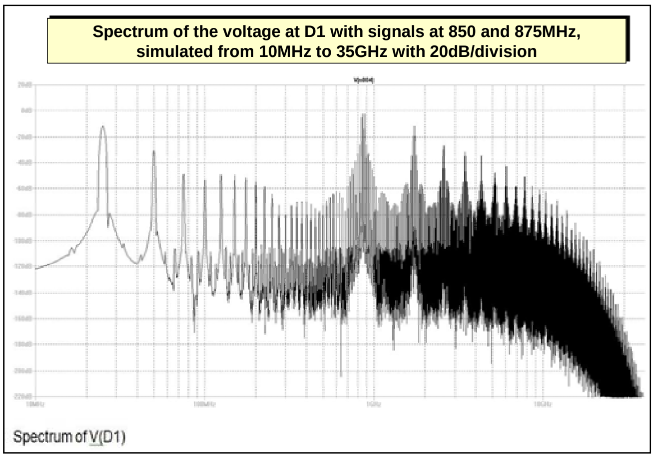

Figure 4 Simulated voltages at D1 in Figure 2

Modulation frequency and type is also an issue for increasing RF immunity test coverage, and some avionics manufacturers (and others) have developed complex modulation waveforms, such as the “chirp + off/on” method described in [14].

With two or more source frequencies, each could be modulated differently. For example while $f1$ is modulated according to the normal test method (e.g. 1kHz sinewave) $f2$ could be modulated with something different, appropriate to the frequency range, for example 17Hz square wave (to simulate TETRA) around 400MHz, 217Hz (to simulate GSM) from 600MHz to 1GHz, pulse modulation to simulate radars above 1GHz, always using the appropriate mark/space requirements.

Also, it is a good idea to have a 0.5sec RF-OFF period for both $f1$ and $f2$ at the same time, at the end of every $f1$ frequency step, to simulate transmitter keying, as recommended in clause A.4.3.10.4.2 of [11]. This should be a “hard” on and off, not ramped up/down.

The reader will appreciate that there is a huge scope, even with just two source frequencies, to achieve much better test coverage of a real-life EME than the usual tests, without changing anything at all about the details of the set-up in the RF test chamber – the most contentious parts of the test methods.

It is possible – by increasing test time a little – to achieve even better test coverage.

When using two RF signal sources as before, step $f1$ through the range as usual (e.g. 0.1% of previous frequency) but add the following $f1$ frequencies where not already covered:

$f1 = f2 - f_{SUS}$, where f_{SUS} is given by:

1) The centre frequencies of any analogue channels (e.g. audio, video, etc.)
2) Any sampling frequencies for A/Ds, D/As, etc.
3) All clock frequencies that are smaller than $f2$
4) The mechanical, hydraulic, pneumatic, etc. resonances of any sensors or actuators (which may only be a few Hz or tens of Hz)
5) The electrical resonances of the circuits and their interconnecting conductors

This will ensure that there are 1st order IM products occurring within the EUT at frequencies that are most likely to be detected during the test because of their effects on functional performance.

The same approach can be applied to the IEC 61000-4-6 test and other conducted RF immunity test methods by feeding the RF PA output into their Coupling-Decoupling Network (CDN), Bulk Current Injection (BCI) clamp, or other type of RF injection transducer.

The above has described tests essentially to IEC 61000-4-3 and 61000-4-6, but there would be no essential difference in applying the proposed method to:

- IEC 61000-4-20 (TEM cells)
- IEC 61000-4-21 (reverberation chambers),
- ISO 11452, methods -2 to -7 and (draft) -9
- ISO 11451, methods -2, -3 and -4
- MIL STD 461F, methods CS114 and RS103
- DEF STAN 59-411, methods DCS02 and DRS02
- RTCA DO160F, Section 20, methods CS and RS

One of the authors outlined this proposed method at the British National Committee GEL/210/12 meeting at BSI Headquarters in London, UK, on 15 Sep 2010. The delegates to that meeting made the following comments about its repeatability issues:

- Non-linearities in the chamber response could cause IM products to occur in the chamber itself and will vary between chambers (ditto for amplifiers, connectors and antennas).
- Different frequencies will resonate at different spots in the chamber, varying their amplitude spatially – hence different “hot spot locations” per frequency.
- The amplitude of the IM products that would appear in the EUT will be very sensitive to the levels of the source signals, for example a 3dB variation in an RF level means a 6dB variation in its IM product.

These issues will make it more difficult for the proposed test to achieve repeatability, than normal single-source-frequency RF immunity tests in one chamber, and will create worse than the usual repeatability between chambers.

Although it is important to reduce test repeatability and measurement uncertainty by as much as is practical, the fact that the proposed test method will probably be less repeatable than the "normal" single-RF-source tests should be outweighed by its considerably increased test coverage – important for increasing confidence in safety and high-reliability applications.

Increasing the levels of the RF sources should help reduce the consequences of the above effects, so the risk of over-testing and/or over-engineering is probably not as significant for EUTs that must operate with high reliability to control safety, financial or other risks.

The significance of the first two bullets will be reduced by testing in reverberation chambers instead of anechoic chambers or TEM cells. Using certain kinds of conducted tests instead of radiated should also improve repeatability.

The GEL 210/12 delegates also asked why use a single *f2*? Why not (for example) use a comb frequency, or a broadband (simultaneous, e.g. white noise) source? The RF PA's power rating will double for every doubling in the number of source frequencies, if they are all at the same level, and would need to be considerably increased with a broadband source.

However, there are ways of generating powerful broadband RF noise sources other than amplifying a small signal, and they could be coupled directly into the antenna feed, although ensuring repeatable frequency responses might be more problematic with such sources.

Reverberation chamber testing could use any number of sources each with their own RF PAs and antennas, significantly reducing concerns over intermodulation in those items.

IV. CONCLUSIONS

Intermodulation between two or more RF sources is a real-life phenomenon that can cause interference in electronic circuits. The present RF immunity test methods only test with a single frequency, and so cannot predict what will happen when the tested equipment or system is exposed to two or more RF sources – as it can be in most real life environments.

This paper has described a proposed development of the single-frequency RF immunity test methods, along the lines already used in some military antenna intermodulation tests.

The aim of the proposed test development is to increase the coverage of RF immunity tests, to help increase the confidence in the verification and validation of the safety and other risks that depend upon the reliability of electronic equipment and systems in real life.

At the time of writing the authors have not tried out the proposed method, but there appears to be every reason why it should work as intended without a significant increase in the time or cost of the tests.

REFERENCES

[1] Prof. Shuichi Nitta, "A Proposal on Future Research Subjects on EMC, From the Viewpoint of Systems Design", IEEE EMC Society Newsletter, Special 50th Anniversary Section: "The Future of EMC and the EMC Society", Issue 214, Summer 2007, pages 50-57, http://www.emcs.org.

[2] Marcel Van Doorn, "Towards an EMC Technology Roadmap", Interference Technology's 2007 EMC Directory & Design Guide, pages 182-193, www.interferencetechnology.com

[3] IEC 61508 (in seven parts), "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems", IEC basic safety publication, http://webstore.iec.ch

[4] Keith Armstrong, "Including EMI in Risk Assessments", 2010 IEEE International EMC Symposium, Fort Lauderdale, FL

[5] Keith Armstrong, "Why EMC Immunity Testing is Inadequate for Functional Safety", 2004 IEEE International EMC Symposium, Santa Clara, August 9-13, ISBN 0-7803-8443-1, pp 145-149. Also: Conformity, March 2005, available: www.conformity.com/artman/publish/printer_227.shtml.

[6] Keith Armstrong: "EMC for the Functional Safety of Automobiles – Why EMC Testing is Insufficient, and What is Necessary", 2008 IEEE International EMC Symposium, Detroit, August 18-22, ISBN 978-1-4244-1699-8 (CD-ROM)

[7] The IET, "EMC for Functional Safety", Edition 1, August 2008, available: www.theiet.org/factfiles/emc/emc-factfile.cfm or www.emcacademy.org/books.asp

[8] Tim Williams, "RF Emissions of Powerline Ethernet Adaptors", The EMC Journal, Issue 82, May 2009, pp 15-18, www.theemcjournal.com

[9] Keith Armstrong, "Why Increasing Immunity Test Levels is Not Sufficient for High-Reliability and Critical Equipment", 2009 IEEE International EMC Symposium, Austin, TX, August 17-21, ISBN (CD-ROM): 978-1-4244-4285-0

[10] "The First 500 Banana Skins", Nutwood UK, Oct. 2007, a compendium of anecdotes, reports, etc., on EMI incidents, from www.emcacademy.org/books.asp (or read on-line at www.theemcjournal.com)

[11] MIL STD 461F, 10 December 2007, "Department of Defense Interface Standard – Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment"

[12] A. Duffy, A. Orlandi, H. Nisanchi, K. Armstrong, "Signal Integrity Testing Using Multiple Out-Of-Band Sources in a Reverberation Chamber", 2008 IEEE Int'l EMC Symp., Detroit, 18-22 Aug., ISBN 978-1-4244-1699-8.

[13] A. Duffy, A. Orlandi, K. Armstrong, "Preliminary Study of a Reverberation Chamber Method for Multiple-Source Testing using Intermodulation", IET Sci. Meas. Technol., 2010, Vol. 4, Iss. 1, pp. 21–27, doi: 10.1049/iet-smt.2009.0008

[14] Keith Armstrong, "Validation, Verification and Immunity Testing Techniques for EMC for Functional Safety", 2007 IEEE International EMC Symposium, July 9-13, Honolulu, ISBN: 1-4244-1350-8.

Presented by Keith Armstrong at the IEEE 2011 Int'l Symposium on EMC, Long Beach, California, August 15-19, ISBN: 978-1-45770810-7