Non-Standardized Immunity Test Techniques to Help Manage Risks caused by EM Disturbances

Dr. William A. Radasky, PhD, P.E.  Metatech Corporation, California, USA  wradasky@aol.com
Keith Armstrong  Cherry Clough Consultants Ltd, U.K. keith.armstrong@cherryclough.com

Abstract – Where electronic equipment must achieve very low risks in Functional Safety or other applications, it is not practicable to rely solely on immunity testing, at whatever test levels, to demonstrate that risks caused by electromagnetic (EM) disturbances are low enough. However, immunity testing to the normal standards is an important part of such equipment’s verification and validation, and using non-standardized immunity testing can help make a good case that the risks caused by EM disturbances are low enough. This paper describes a number of ways in which the standard test methods can usefully be modified, for this purpose.

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

I. INTRODUCTION

Where electronic equipment must function so as to maintain acceptable levels of functional safety risks, or low levels of other types of risks (e.g. financial, reputational, etc.), it is not possible to rely only on immunity testing to standards – however high the test levels used – to demonstrate that risks caused by electromagnetic (EM) disturbances are low enough, as discussed in [1] [2] [3] and [4].

However, being able to pass the relevant immunity test standards throughout the lifecycle is important for maintaining the availability of the equipment, to help prevent users or owners from disabling safety-related systems which too often shut down their “equipment under control” (EUC) because they don’t have sufficient immunity to the EM disturbances they experience in real life, see [3] and 8.1.1 in [6].

Because electromagnetic interference (EMI) is a “systematic” type of failure (instead of a random one) the IEC’s Basic Standard on Functional Safety IEC 61508 [7] requires sufficient “design confidence” to be achieved to show that the proportion of the risk budget allocated to risks caused by EM disturbances is not exceeded [4], and immunity testing that goes beyond the relevant EMC standards can help to provide such confidence. An example is where redundant systems (multiple channels operating in parallel, with comparison or voting on their outputs, see 8.2.2 in [6]) use different technological implementations to help ensure that EM disturbances will not interfere with all the channels at once, see 6.3 and 6.4 in [6].

The following sections briefly describe a number of non-standardized immunity test methods, usually based on standardized test methods, which can be helpful as part of the verification/validation of equipment used in low-risk applications.

II. WHERE SIMULTANEOUS EM DISTURBANCES COULD AFFECT THE SAME CIRCUIT NODES

Passing all relevant immunity tests using higher levels than can occur in real life helps deal with the simultaneous EM disturbances that will occur in real life, for example:

- Two or more radio channels at significant levels.
- One or more radio channels plus a transient, surge, or ESD event.
- Two independent transients, or a transient plus a surge, overlapping in time. Such overlaps can occur more often than is acceptable for the risk level.

Ron Brewer says, in [8]: “…there is no way by testing to duplicate all the possible combinations of frequencies, amplitudes, modulation waveforms, spatial distributions, and relative timing of the many simultaneous interfering signals that an operating system may encounter. As a result, it’s going to fail.” He goes on to recommend testing all possible EM disturbances at higher levels than can occur in the environment, while recognizing (as does [2]) that such testing cannot, alone, prove that acceptable risk levels will be maintained. The whole point of the approach in [6] and [7] is to ensure that when (not if) it fails, it remains safe enough.

Michel Mardiguian showed in [9] that equipment that passed individual immunity tests at the maximum specified levels would not pass when two tests were applied at the same time with both at maximum levels. For example, with the maximum RF field applied, EFT/B could only be applied with very low levels. Like [8], [9] went on to recommend performing the regular immunity tests with higher test levels than were needed for the relevant type of EM disturbance alone. It is instructive to analyze what is going on, and why it is that increasing the test levels on individual immunity tests can be useful for dealing with simultaneous EM disturbances. This approach is valuable where different types of EM disturbances (say, conducted continuous RF, and EFT/B) are capable of coupling noise into the same circuit node.

Digital designers ensure systematic noise is below the logic threshold by an amount called the “noise margin”, so that ambient noise (i.e. inter-system noise) does not add to it by enough to cause the logic 0 state to exceed the logic threshold and appear to be a logic 1 state – known as a “bit flip”.

This paper was first published by the IEEE EMC Society as part of their 2016 International Symposium on EMC and Signal Integrity, Ottawa, Canada, 25-29 July 2016. Please respect the IEEE's Copyright on this paper.
Figure 1  Logic 0 during continuous immunity test

Figure 1 shows an example of a logic 0 state whilst equipment is being immunity tested with continuous radiated or conducted RF (e.g. to IEC 61000-4-3 or -6). This sketch shows the systematic (self-generated) noise floor plus the demodulated envelope of the coupled RF, and in reality, with a linear vertical scale, the systematic noise would also be visible on top of the demodulated sine wave noise.

Designers usually aim to just about comply with the RF immunity specifications in the relevant EMC standards, to keep costs low. So we could say that the noise in the logic signal during each immunity test: “just about uses up the entire noise margin”.

Figure 2 shows a logic 0 state during a fast transient burst immunity test (e.g. EFT/B to IEC 61000-4-4). Once again, the noise caused by the immunity test “just about uses up the entire noise margin”.

Figure 3 shows the equipment subjected to the continuous RF and EFT/B disturbances (Figures 1 and 2) at the same time. Now there are occasions when the overall noise level exceeds the logic 1 threshold, when the logic 0 state can be mistaken for a logic 1 state, and an error can occur. Logic 1 signals can be mistaken for logic 0 in the same way, for the same reasons (to visualize, just invert Figures 1 to 3). These three figures show that – to allow for noise levels in circuit nodes building up due to two or more simultaneous EM disturbances – when testing immunity with individual EM disturbances the test levels for each test should be set to be equivalent to the foreseeable combined noise level in the equipment’s operational EM environment over its lifecycle.

Figure 2  Logic 0 signal during EFT/B test

Figure 3  Logic 0 during RF and EFT/B testing

Similar arguments to the above also apply to testing analog systems, when the signal-to-noise ratio at each circuit node must remain less than a specified level, for correct operation.

Assessment of the application’s EM environment might reveal that equipment needs to cope with three or more simultaneous EM disturbances at significant levels, for example:

- Three or more radio channels at significant levels (e.g. cellphones, Wi-Fi, M2M, RFID, etc.)
- Two or more radio channels at significant levels plus a transient burst, surge, or ESD event
- One or more radio channels plus two or more independent transients or surges that overlap in time

In such EM environments, individual immunity test levels may need to be set even higher than double the maximum levels expected for each individual type of disturbance. So-called “exclusion zones” have for decades been used in the hope of protecting equipment from RF fields higher than they have been tested for, but are not recommended these days [10] because, to work as intended, they:

a) Must be faithfully observed by users and third-parties, and so should not be expected to provide a risk-reduction of more than 50%

b) Must restrict the number of nearby mobile/portable transmitters to one, which might have made sense in the 1990s but not these days

Where the above would require increases in test levels, it seems to the author that their individual, independent levels should be added linearly. So if the maximum possible number of nearby transmitters was four, and each could cause 30V/m, we would test with 120V/m over the entire radiated frequency range. More sophisticated analyses based on the digital modulation characteristics and channel occupancies of the
transmitters would probably allow reduction of this test level. We know from [11] that some computers and computer networks might not function reliably at such levels – but we also know that certain automotive and aerospace electronics normally pass tests at such levels, sometimes much higher.

But increasing the levels of ESD, EFT/B and surge tests to allow for the possibility of simultaneous EM disturbances, can soon reach voltages that cause non-linear effects (e.g. flashover, component damage, etc.) in the EUT which would never occur in real life and so such tests would not increase confidence in the design. It might be considered reasonable to increase them to high levels have sometimes been reported or may be theoretically possible, and coping with them might help prove equipment suitable for some applications. Indeed, in some situations (e.g. high exposure to lightning, EMP, space vehicles, etc.) even these transient, surge and ESD levels might be considered too low.

Where non-linear effects are a concern, sufficient design confidence might be achieved by testing like Michel Mar-diguijan did in [9], by performing two different immunity tests at the same time, taking care to ensure that the immunity test equipment associated with each test is grossly affected or damaged by the other test. But where it is impractical to increase the individual test levels by enough, or non-linearities would make the results meaningless, and simultaneous immunity tests are impractical, simultaneous EM disturbances are probably best not dealt with by testing, instead using the well-proven techniques in design, verification and validation described in [4] and the publication it is based upon, [6].

III. WHERE EM DISTURBANCES COULD AFFECT DIFFERENT CIRCUIT NODES

In a given equipment or system, some circuit nodes could be more sensitive to some types of EM disturbances than others. For example, an analog signal amplifier could be especially sensitive to continuous EM disturbances, whilst a digital processor could be especially sensitive to ESD impulses, and a power converter could be especially sensitive to surges. In such situations, real-life exposure to different types of EM disturbances might increase risks by too much, but would never be discovered by testing with just one type of EM disturbance at a time.

Another issue is that some types of conducted real-life EM disturbances will affect two or more ports at the same time, possibly causing two or more simultaneous upsets in different circuits that could lead to dangerous errors or malfunctions. But because the standard tests apply these disturbances to one port at a time, they might not discover the real-life risks.

It may be practical to cover some of the above situations by testing two or more ports with the same, or different, EM disturbances at the same time (see [12]) – but, in any case, the following method is strongly recommended:

a) During all immunity tests, including non-standardized tests described in this paper, monitor and record in sufficient detail the performance of all circuits which could play any part in creating unacceptable levels of risk, even where the performance degradations do not themselves cause problems.

b) After all the tests are complete, analyze the complete set of results to see whether any combinations of the performance degradations that have been recorded could possibly lead to unacceptable risks, even if they do not occur at the same time.

For example, if radiated fields at one frequency cause one redundant channel to malfunction, whilst a different frequency causes a different redundant channel to malfunction, then a “two-out-of-three redundant” system would fail if those two frequencies occurred simultaneously at high-enough levels, which is of course a real-life possibility.

Another example: if a fast transient burst could cause a process vessel to open its inspection valves and release a hazardous gas into its surroundings (as has happened with chlorine) and if the gas detector that should trigger emergency ventilation could be inhibited by a radiated field, or switched off by an ESD event, then some combination of those EM disturbances – not necessarily at the same time – could allow a hazard to occur.

IV. MODULATION FREQUENCIES THAT A DESIGN IS ESPECIALLY SUSCEPTIBLE TO

Electronic equipment tends to be especially susceptible at the operating frequencies of its internal hardware and software processes (see [13]). For example, it is commonly observed during continuous RF testing that synchronous-processing (i.e. clocked) digital circuits are most likely to suffer problems in narrow frequency ranges around the frequencies of its clock and/or some of its harmonics. Often, these will be the clock-related frequencies that are most evident in the emissions tests.

One of the authors has been involved with two situations where different types of equipment passed tests with any radiated frequency at 100 V/m or more with 1 kHz sine-wave amplitude-modulation – but were at least 80 dB more susceptible over wide ranges of carrier frequencies when the sine-wave modulation was changed to one of their circuits’ operating frequencies. Both situations were discovered by accident during testing with the 1 kHz square-wave (i.e. pulse) modulation specified by their customers, because – quite by chance – their especially-susceptible frequencies were very close to a harmonic of the square-wave modulation. Both used AC-energized sensors, and both would cause severe financial and/or safety problems if interfered with in normal operation. These real-life examples shows that some circuit designs can be very susceptible indeed at certain frequencies, whether these result from carrier-waves, demodulated RF envelopes, or intermodulation. It seems to be the case that some safety-related electronic systems only remain safe-enough as long as certain specific frequencies (or modulations) do not occur in their operating environments.

To deal with this issue, certain safety-related industries use a continuous RF test method in which carrier waves are conducted and/or radiated whilst being stepped in small incre-
ments from 0 to 30kHz, with a one-second pulse OFF then ON again at each step (i.e. 0.5Hz pulse modulation). Note that some test methods (e.g. IEC 61000-4-16) only use common-mode noise injection, whereas differential-mode injection may also be required to better simulate the effects of EM environment on the equipment. When the CW frequency exceeds 30kHz, each frequency step has an unmodulated period, followed by 'chirp' modulation from 0 to 30kHz, followed by an OFF period of one second and then switched ON again, unmodulated, ready for the next frequency step. Such 'CW, chirp, plus OFF/ON' tests must be slow enough to be sure of detecting any errors, malfunctions or damage given the response times of the functions being monitored. If necessary, time may be able to be saved by monitoring critical internal signals to avoid having to wait for long time-constants to respond. Special fiber-optic and other probes are available for such monitoring, but careful test planning might avoid the need to use them.

If the 'especially susceptible frequencies' have previously been identified (see [13]) the testing time can be reduced by modulating only with those frequencies instead of the chirp. A method of identifying these frequencies not mentioned in [13] is to measure the emissions over a wide frequency range (e.g. 10Hz to 10GHz), not necessarily using standard test methods, and analyzing the results to identify the repetitive electrical activities in the EUT that caused them. With the addition of the bandwidths of any baseband analogue processing (which don’t produce emissions), these will probably be the most susceptible frequencies.

MIL STD 461 [14] and RTCA DO-160 [15] have both long-recommend performing RF testing with frequencies and modulations that equipment is especially susceptible to, so the author cannot claim any credit for suggesting this modification to the usual conducted and radiated immunity tests.

V. INTERMODULATION

Figure 4 shows the effect of two frequencies, chosen as 400 and 500 MHz for simplicity, on a semiconductor device. The two frequencies are rectified by non-linearities in the semiconductor to generate baseband noise (the sum of the demodulated envelopes) plus harmonics of the two original signals. Harmonics above the 2nd occur, of course, but are outside the scale of Figure 5 and so not shown on it.

The semiconductor non-linearities also cause mixing (heterodyning) of the two signals, creating sum and difference frequencies, in this simplistic example, at 100MHz and 900MHz. These are called “1st-order Intermodulation (IM) products”, and with just two initial frequencies there are only two of them. However, the original signals’ 2nd-order harmonics also intermodulate with each other; with the original signals, and with their 1st-order IM products, creating “2nd-order IM products” at 2f2 – f1, 2f2 + f1, 2f1 – f2, 2f1 + f2, 2f2 – 2f1 and 2f2 + 2f1 – six of them from two initial frequencies, only a few of which can be shown within the frequency range of Figure 4. 2nd-order IM products are generally lower in level than 1st-order products.

Next, the 3rd-order harmonics of the two original frequencies interact with the 2nd-order and 1st-order IM products, and also with the original two signals, giving a large number of 3rd-order IM products, generally at a lower level than the 2nd-order products, and so on with the 4th, 5th, 6th, etc., IM products. Figure 4 only shows IM products up to the 2nd-order, but the two signals at 400 and 500MHz would actually create dozens of IM products – new frequencies which were not present in the EM environment.

Imagine we are in a regular EMC test laboratory, performing regular RF immunity tests with a single carrier frequency. When tested over, say, 10 kHz to 10 GHz, we might find the equipment under test (EUT) to be especially susceptible over the range 50 MHz to 100 MHz. Being good EMC engineers, we add filtering and shielding that is effective over the range 10MHz to 200MHz, 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 expected not to increase manufacturing costs by any more than necessary so we do the minimum we have to, to pass the regular EMC tests. 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. However, real life EM environments generally have two or more frequencies above 500 MHz at significant levels, and the 10MHz – 200MHz filtering and shielding improvements will not keep them out of the equipment. They will intermodulate (i.e. mix, heterodyne) within its semiconductors creating IM products that can easily fall within its especially susceptible 50 MHz to 100MHz region – possibly causing errors, malfunctions or faults that increase risks by too much.

IM products have lower levels than the frequencies that caused them, but susceptible frequencies can be very sensitive indeed, as the two 80+ dB real examples earlier show. 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 29/2 - 18/1, that would be expected to arise in the semiconductors but at quite a low level. Single-frequency testing at any level will not discover this real-life susceptibility to IM products (see [2]), so the following “twin-tone” test method is recommended, very similar.
indeed to the antenna intermodulation and “cross-modulation” test methods CS103 and CS105 in MIL STD 461F [14] [16].

Two (or more) frequencies $f_1$ and $f_2$ are combined (e.g. by a resistive summing circuit), amplified and – for radiated tests – input into an antenna that illuminates the EUT in a test set-up that otherwise follows the chosen immunity test method (e.g. IEC 61000-4-3) as closely as is practical. This twotone test can also be used for conducted RF immunity tests (e.g. IEC 61000-4-6). $f_1$ is swept as required by the immunity test, with $f_2$ initially set to twice $f_1$'s start frequency. When $f_1$ reaches $f_2$, $f_2$ is doubled, and this process is repeated up to the maximum value of $f_1$. For example, if $f_1$ is to cover 80MHz to 3GHz, $f_2$ is initially set to 160MHz, then 320, 640, 1280, 2560 and finally 3000MHz.

This “twin-tone” RF test signal will generate IM products in semiconductors and other non-linearities in EUTs, without increasing the test time. There are issues associated with antenna (or other transducer) bandwidth, amplifier power, and the frequency response of the test chamber, but none of these are difficult for a competent test engineer to deal with, especially when one understands that one is not performing a standardized immunity test but a non-standard test in an attempt to find design flaws that could cost lives, or have other very undesirable results. For more information on IM testing, see [17].

VI. MORE ANGLES/POLARIZATIONS IN RADIATED TESTING

Anechoic testing is unlike most real-life radiated EM environments, and small changes in angles of incidence have been seen to cause susceptibility variations of 30dB or more, so Reverberation Chamber methods have been developed to give more confidence [18] [19] [20] [21]. A ‘reverberation chamber’ test method currently used for some safety-critical systems rotates the chamber’s ‘stirrer’ or ‘paddlewheel’ over a full revolution, in between 20 and 120 angular steps. At each step of the paddlewheel, radio fields are generated in the chamber, comparable in frequency range and magnitude with the foreseeable worst-case EM environment(s). The frequency range is covered in small steps (e.g. 0.1%). At each frequency step the field is modulated with the appropriate signal. Some safety-related industries use the “CW, chirp plus OFF/ON pulse” briefly described in Section IV, and the twotone method briefly described in section V, or other complex modulations could be used instead, or as well. For more on reverberation chamber testing for Functional Safety, see [22] and [23].

VII. INCREASED FREQUENCY RANGES (LOWER AND HIGHER)

Real-life EM environments can contain significant levels of EM disturbances outside the frequency ranges specified by the regular immunity tests. So it helps improve design confidence if the continuous RF immunity tests are performed over wider frequency ranges, whether they are the regular standardized tests or non-standardized tests including (but not limited to) those briefly described in this paper

VIII. COMBINING EMC WITH ENVIRONMENTAL TESTING

Shock and vibration, bending forces, temperature extremes or cycling, wear, and many other lifetime mechanical, physical, climatic and biological influences can affect the radiofrequency (RF) stability of some types of circuits, and degrade the performance of EM mitigation measures such as shielding, filtering and transient suppression, for example by corrosion, over a lifecycle. There are well-established test methods for most physical phenomena, and “HALT” test experts combine physical test methods to quickly discover likely end-of-life characteristics. But some physical stresses might occur that are not covered by established standards, for example the use of abrasive cleaners, or the repetitive opening and closing of a door or inspection panel, so it is helpful to devise realistic tests for such physical lifetime stresses. As mentioned earlier, many manufacturers ignore the valuable information that can be obtained by retesting equipment for immunity after its HALT tests are completed and comparing the results with what it achieved when new.

However, this does not provide any information on the temporary effects of physical stresses such as mechanical forces, temperature extremes, etc., for example causing joints in shielded enclosures to open, filters to degrade as their inductors approach their Curie points, etc. Where electronics
are protected from the physical environment by an external means, such as an enclosure, physical tests can be carried out on the enclosure, as shown in Figure 6 while its shielding effectiveness is measured. These measurements are made in the environmental testing suite so the EM environment will be noisy, but this can be worked around by using tracking generators, or “comb generators” with precisely known frequencies, to establish the fields inside the enclosure. Alternatively, close-field probes could be glued to the enclosures seams, joints, cable penetrations, etc., instead of using an antenna as shown in Figure 6. For more on this, see [24].

IX. SLOWLY VARYING THE SUPPLY VOLTAGE FROM ZERO

Power supply dips, dropouts and variations can be outside the range tested by the standard immunity tests, so it is helpful to extend their range (just as Section VII recommended extending the standard frequency ranges). However, one useful technique that is used by certain functional safety assessors is to use a variable power supply to slowly increase the external power from zero up to the nominal supply voltage, and then to slowly reduce it back to zero. This is often done under manual control, taking a minute or longer to complete. During this test the EUT should either work correctly, or shut down correctly, but it is not unusual to find unspecified behaviors appearing which might cause unacceptable levels of risk in real-life applications.

X. CONCLUSIONS

Many different types of non-standardized immunity testing can readily be devised and performed by competent EMC test engineers, often by simply extending and/or modifying the standard tests, to help provide sufficient confidence that a given design should not cause unacceptable levels of functional safety or other risks as the result of real-life EM disturbances over its lifecycle.

REFERENCES

[18] IEC 61000-4-21, “EMC testing and measurement techniques – reverberation chamber test methods”.