emc STANDARDS

Another EMC resource
from EMC Standards

Why increasing immunity test levels is not sufficient for high-reliability and critical equipment

Helping you solve your EMC problems

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

Why increasing immunity test levels is not sufficient for high-reliability and critical equipment

Keith Armstrong
Cherry Clough Consultants
keith.armstrong@cherryclough.com

***Abstract* – It is often assumed that passing an EM immunity test at 100% of the level of the worst-case disturbance that can occur over the lifecycle, and taking measurement uncertainties into account, will prove that the design of the tested equipment will almost never suffer from errors or malfunctions due to that disturbance in real life.**

Unfortunately, although the above is *necessary* when testing the EM immunity of equipment that must function with high reliability – such testing is *insufficient* to demonstrate that high-reliability, security, mission-critical or safety-critical equipment or systems will achieve tolerable failure levels over their lifecycles despite the EM disturbances in their environments.

Part II of this paper explains why this is so, and Part III briefly introduces the techniques that are necessary for achieving sufficient confidence in EMC, when high reliability is required.

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

I. INTRODUCTION

Electronic circuits of all types, and the software or firmware that runs on digital electronic circuits, are susceptible to errors and malfunctions caused by electromagnetic interference (EMI) from the electromagnetic (EM) disturbances that can occur in their environments. Clause 6.1 and Table 3 of [1] and Annex B of [14] reviews the many types of EM disturbances that can occur.

As integrated circuits (ICs) are fabricated with ever-shrinking silicon features [2] and run on ever-lower voltages, their susceptibility to EM disturbances increases. This means that electronic equipment that uses ICs requires ever-increasing efforts in design, and increasing costs in manufacture, to achieve given levels of reliability in real life operation.

(The word ‘equipment’ is used here in its widest context, to include systems and installations of any complexity or size.)

The result of not achieving adequate immunity to the EM disturbances that can occur in the real-life environment, is (for the manufacturer) high levels of warranty costs and (for the user) high levels of downtime. Getting EM immunity wrong can be very costly indeed and has even led to the demise of some companies [3].

This problem is most keenly felt where the reliable operation of electronic circuits (and software/firmware) must be the highest, for example in ‘high reliability’, ‘mission-critical’, ‘safety-critical’ or security applications. Some electronic equipment used in such applications might need to have a mean-time between failure (MTBF) as high as 100,000 years, for economic or safety reasons (equivalent to SIL 4 in [4]), for example the control of the safety shutdown of a nuclear power plant – in order not to expose people to the intolerable risks that would be caused by a core meltdown. Similar examples of high MTBF requirements can be drawn from many other application areas, especially military, security, aerospace and public infrastructures, where an equipment failure could put many lives at risk.

Some would argue that – where equipment is mass-produced and used by large numbers of people at any one time (e.g. automobiles, domestic appliances, etc.) – similar levels of reliability are required even though only a few people are at risk from a failure of an individual item of equipment.

Since the MTBF requirements include failures from a multitude of possible causes, EMI being just one of them, the requirements for EM immunity alone are more stringent.

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

Performing immunity tests with sufficient repeatability to allow one model of equipment to be compared with another, requires detailed specifications for test equipment, test set-up and test methodology. As a result, various industries and standards bodies have, over the years, created EM immunity test standards. Examples include military [5]; civil aircraft [6]; medical [7]; industrial, commercial and consumer [8]; telecommunications [9] [10] and automotive [11] [12] [13].

EM immunity testing is a costly and time-consuming business, and some of the test facilities that exist are very large and impressive, and cost several million dollars.

Many scientists and engineers have spent almost their entire careers in dealing with the complexity of the test standards; the creation of the facilities for performing the tests; in actually doing such testing; and in designing equipment so that it passed the tests. The numbers of conference papers published worldwide on the above topics alone, numbers many thousands annually.

All this detail, effort, time and cost should not obscure the fact that EMC immunity testing is incapable, *on its own*, of demonstrating that high levels of reliability will be achieved over the lifecycle of an equipment. Even if the test levels are increased by 6dB (or more) over the normal maximum levels.

Assessing the worst-case EM disturbances

A simplified and earlier version of this paper (6 pages) was published in the Proceedings of the IEEE International EMC Symposium, Austin, TX, August 17-21, 2009, ISBN (CD-ROM): 978-1-4244-4285-0.

In some industries, such as military and flight-critical avionics, the maximum levels of EM disturbances that can be experienced in their environments are measured by comprehensive and costly surveys that take many years and are continually updated. These levels are then taken into account by the test standards, in the test levels to be applied.

But the test levels applied by most other immunity standards, including all of the industrial, commercial and domestic ones in the IEC 61000-4 series [8], are based on undisclosed "economic/technical compromises".

It is often claimed by the committees who produced [8] that their maximum test levels cover about 80% of amplitude range likely to be experienced by equipment over the lifecycle. This means that chances of an EM disturbance exceeding the tested levels, and possibly causing an error or malfunction, is about 20%. This figure compares very poorly with the reliabilities typically required for high-reliability and mission/safety-critical equipment, never mind the 100,000 year MTBF example mentioned earlier.

For an immunity test to be able to provide any confidence that high reliability has been achieved, its test levels must correspond to the maximum levels that can be experienced during real-life operation of the equipment. A thorough program of environmental monitoring, complemented (where necessary or useful) by calculations based on the characteristics of the known or foreseeable sources of EM disturbances and their propagation characteristics, can provide such data.

Such a program often results in probability distributions, which can be used to decide what EM test levels should be used, based on the reliability (e.g. MTBF) required. A good example of this is the work that has been done on lightning over the decades, allowing lightning tests to be performed with impulse levels set to provide the required confidence in surviving lightning events over the lifecycle, which vary depending on the geographical region concerned.

Unfortunately, outside the military and aerospace industries and the lightning world, the necessary EM environmental surveys have not generally been performed. So equipment specifiers have some work to do, to establish what levels to test to, if they want their equipment to have high reliability.

Clause 6.3 of IEC/TS 61000-1-2 [1] spends half a page describing a "*Methodology to assess the electromagnetic environment*" intended to establish the 'maximum level' for each significant EM disturbance, to be used in specifying the immunity requirements. Steps 1 and 2 in the IET's 2008 guide [14] spends 25 pages describing this in more detail. [15] and [16] may also be of interest.

In many cases, this methodology does not reveal the probability distributions of the disturbances' amplitudes – so the usual approach is to test at the level of the highest reasonably foreseeable disturbances, sometimes called the 'worst-case' levels, that could occur during the lifecycle.

Taking measurement uncertainty into account

Assuming the worst-case EM disturbances over the lifecycle are known or have been reasonably foreseen, the quest for proving reliability by immunity testing then has to deal with the issue of measurement uncertainty. There are uncertainties in measurements of the EM environment, and uncertainties in the measurements of the EM disturbances applied during immunity testing.

So to improve the confidence achieved by immunity testing, it is usual to allow for these uncertainties by increasing the test levels by an amount, often called a 'margin' (sometimes, confusingly, a 'safety margin'), above the worst-case level that could occur in the environment over the lifecycle.

For example, [5] requires: "*Safety critical and mission critical system functions shall have a margin of at least 6 dB. EIDs shall have a margin of at least 16.5 dB of maximum no-fire stimulus (MNFS) for safety assurances*…" (EIDs are electrically initiated devices, basically detonators for pyrotechnics and munitions). The author understands that these margins are based on a thorough understanding of the uncertainties associated with the measurements of EM disturbances, and the margin of 16.5dB also takes into account the range of the stimulus required to fire a given type of EID, due to manufacturing variability.

6dB seems to have become widely established as a suitable margin whenever high reliability is required. But the correct margin to use depends upon the reliability required for the equipment, and should be calculated anew for each EUT and each measurement using the method of 'expanded uncertainty' as described in [17].

Assume that the probability distribution of the disturbance level applied by an immunity test (its overall measurement uncertainty) has a symmetrical shape. In this simple case, testing exactly at the specified level means that the actual test level applied to the EUT is 50% likely to be below the specified level, and 50% likely to be above. So the test only achieved a 50% confidence that the EUT was actually tested at the specified level or higher.

Assuming a 'Normal' (Gaussian) distribution for the measurement uncertainty – as sketched in Figure 1 – we can use the expanded uncertainty method in [7] to improve the confidence that the actual test level applied to the EUT equaled or exceeded the specified level.

Increasing the test level by a margin equal to one standard deviation (1σ) achieves 68.3% confidence that the actual test applied the specified level, or more, to the EUT. A margin of two standard deviations (2σ) improves confidence to 95.4%, three standard deviations (3σ) achieves 99.7%, and four standard deviations (4σ) 99.99% (i.e. 1 part in 10,000). Margins of up to 5σ (99.9999%) might be required for high-reliability and mission/safety-critical equipment, depending on the likelihood of the threat occurring in real life (and the confidence of that estimation), and the consequences of the system failing.

But although all the above considerations of the level to be used for immunity testing are *necessary*, they can never be *sufficient* for demonstrating that equipment will operate with the required reliability, despite the disturbances in its EM

A simplified and earlier version of this paper (6 pages) was published in the Proceedings of the IEEE International EMC Symposium, Austin, TX, August 17-21, 2009, ISBN (CD-ROM): 978-1-4244-4285-0.

environment over its lifecycle.

Part II explains why this is, and Part III briefly introduces what is required to be able to demonstrate adequate reliability as regards immunity to EM disturbances.

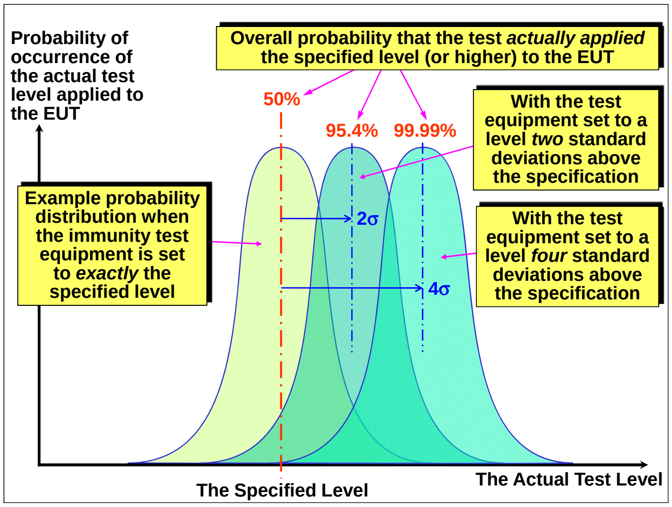

Figure 1 Increasing safety risks due to EMI

Taking degradation of EM characteristics into account

Many EM characteristics degrade with time. For example, shielding effectiveness always degrades as joints fail and gaskets and other electrically contacting surfaces oxidize, corrode through galvanic and/or fretting action, and/or get covered with non-conductive deposits. Over-voltage sure protection degrades as surge protection devices wear out. Filter effectiveness degrades as ground bonds increase resistance or fail due to vibration, and when capacitors are burnt out by overvoltages.

They can also degrade with misuse and/or faults, for example when a grounding conductor fails, or a shielding door or panel is left open.

Increasing the test level can be a way of allowing for some degradation of EM characteristics, but in most cases it cannot make complete provision. It is not at all unusual for mitigation techniques such as filtering, shielding and ESD/surge protection to attenuate the EM disturbance(s) concerned by at least 30dB. Critical military and aerospace equipment sometimes requires as much as 80dB attenuation (or more).

So, for example, if the worst-case levels of E-field that could occur over the lifecycle were 30V/m (which would require cellphones and other portable and mobile radio transmitters to be reliably kept further away than appropriately-specified distances), then testing to allow for the degradation of normal levels of mitigation would need to employ field strengths of about 1kV/m over the frequency range (30dB higher than 10V/m).

At such high field strengths, non-linear effects would be expected, that would not occur with the actual lifecycle worst-case in the situation where the mitigation had degraded due to age, faults or misuse. So such tests would not be representative anyway.

In the case of critical military equipment that could be exposed to 100V/m over its lifecycle, overtesting to simulate ageing, faults or misuse could mean testing at 80dB higher, which would be 1GV/m (many times higher than the breakdown voltage of the air). Clearly an unfeasible test to perform.

When overvoltage testing, testing a surge protection device with a 30dB higher surge voltage than the lifecycle's worst-case, would have quite a different effect than if the equipment was subject to the worst-case level but with the surge protection device open-circuit due to wear-out or a fault. Such tests would require "combination wave" test equipment that had an open-circuit voltage of, say, ±60kV and a short-circuit current of ±66kA (30dB higher than ±2kV and ±1kA).

The above examples assume that the increased test levels allow for the complete loss of the mitigation, which is of course possible over a lifecycle when ageing, damage, faults and misuse are considered. However, regular maintenance of EM characteristics (a common practice for certain military equipment) can control their degradation, keeping it within certain limits over the lifecycle.

So increasing the tested levels can – in some circumstances – be a trade-off between allowing for some degradation, and decreasing the period between maintenance activities that would refurbish the EM characteristics to a known condition.

Some equipment designs might use EMI monitoring devices to detect degradation in EM characteristics, damage faults or misuse. These can help save cost by requiring maintenance or repair activities to be performed only when needed. In such situations there could be a trade-off between increased test levels and the trigger thresholds of the EMI monitors.

II. WHY TESTING AT HIGHER LEVELS IS INADEQUATE

This section discusses several of the reasons why applying the usual types of EM immunity tests, even with test levels increased above real-life worst-cases by margins much greater than 6dB, cannot cover most of the lifecycle reliability issues that could arise through an equipment's exposure to EM disturbances in its environment.

This contradicts the conclusions of [32], which are based on many of the same reasons given below.

Angle of incidence and polarization of the illuminating field

It is commonly assumed that the maximum field penetration of a shielding enclosure (its minimum shielding effectiveness, SE) obtains when the illuminating field has normal incidence, which is why most radiated immunity tests are set up the way they are.

But this assumption turns out to only be valid when there is a single aperture in the illuminated face of the equipment. Most real-life enclosures will have two or more apertures, and [18] shows that the interactions between them can result in greater field penetrations (lower SEs) for non-normal incidence. Similar points are made by [19], [30], [31] and [32].

Figure 2 sketches an example with three susceptible items (A, B, C) located at different places within a shielded enclosure.

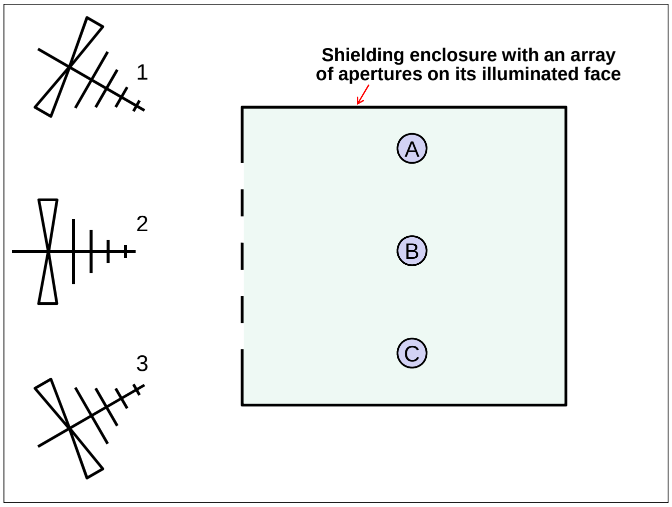
Shielding enclosure with an array of apertures on its illuminated face
1
2
3
A
B
C

Figure 2 Enclosure illuminated from different angles

With normal incidence (illumination by antenna 2) it might be that item B is exposed to the maximum field strength, causing a certain malfunction to occur during the test when the level of the field reaches some critical value. Increasing the test level further might not reveal the possible malfunctions of A and C, because of the prior malfunction of B.

However, non-normal illumination by antenna 1 might create the maximum field strength at location C, so that C malfunctions and 'hides' the possible malfunctions of items A and B, regardless of the test level. Likewise, non-normal illumination by antenna 3 might create maximum field strength at location A, so that A malfunctions and 'hides' the possible malfunctions of items B and C.

Most radiated immunity test methods use anechoic chambers and to save testing time only subject the various faces of the EUT to illuminating fields with normal incidence. As shown above, such measurements may not detect errors or failures that can occur with other angles of incidence, which of course can occur in real-life operation.

Confidence that a radiated immunity test will discover the EUT's full range of errors and malfunctions that could occur in real-life EM environments, *cannot* be achieved by simply illuminating with normal incidence and increasing the test margin by any amount. In this example, it will always be B that fails, and – depending on its failure mode – the failures of A and C could go undetected, or be misjudged.

However, very considerably increased confidence *can* be achieved by testing in a reverberation ('stirred-mode') chamber instead of anechoic, because over the period of the test it illuminates the EUT with a vast range of angles and polarizations. Just the worst-case environmental level plus the expanded uncertainty margin need be applied.

Reverberation chamber testing thus provides very much more confidence that the possibilities for errors and malfunctions in real life have been covered, than it is possible to achieve with the usual anechoic tests with whatever margins. It is recommended by [18], and is the preferred radiated immunity test method in [6].

The most susceptible frequencies

Electronic equipment can suffer errors or malfunctions due to electrical noise that occurs close to certain especially susceptible frequencies, or over certain frequency ranges. These especially susceptible frequencies can often be determined by analysis of circuits, software/firmware, and loads. Examples include:

- A clocked digital processing circuit, or any oscillator, close to its fundamental and its harmonics
- A load transducer, close to its physical resonances (e.g. a vehicle's road wheel or suspension, a pump driving a fluid or gas load)
- The range over which an amplifier's gain exceeds 0dB

Figure 3 shows a simple example of an equipment that contains two items, labeled D and E, that have different especially susceptible frequencies. D is most susceptible at 1kHz, at which frequency it requires a noise level of 0dBm to suffer from an error or malfunction. E is most susceptible at 7kHz, where a noise level of 0dBm will cause an error or malfunction. At 1kHz, E is 20dB less susceptible.

To save time and cost, most standardized radiated immunity test methods use amplitude modulation at 1kHz of the carrier wave, with a modulation depth of 80%.

Assuming that D and E are located physically close together and so are exposed to the same radiated fields inside their equipment's enclosure, then – when testing with 1kHz sine modulation and increasing the test level – D will first suffer interference at a given level, with E immune until the level is increased by 20dB more.

In real life, 7kHz modulation is just as likely to occur as 1kHz, but testing with 1kHz sine wave modulation will hide the potential failure of E in real life, or cause it to be misjudged because it will only occur when there is a failure of D.

So the potential failure of E – which could be more significant than failure of D – will not be reliably detected by testing with 1kHz modulation, whatever the margin.

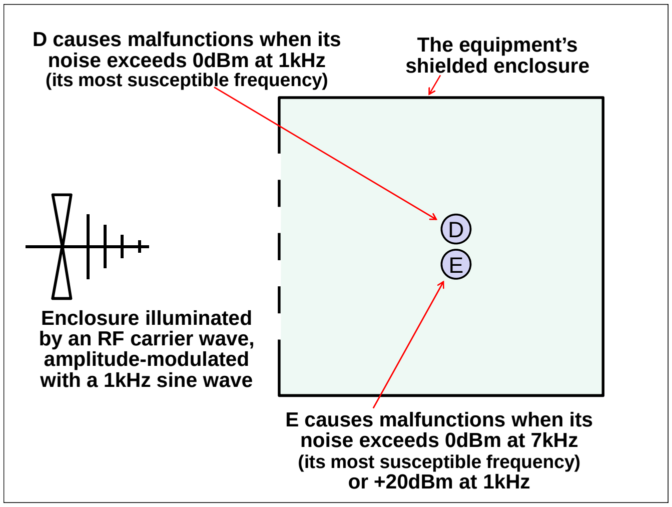
D causes malfunctions when its noise exceeds 0dBm at 1kHz (its most susceptible frequency)
The equipment's shielded enclosure
D
E
Enclosure illuminated by an RF carrier wave, amplitude-modulated with a 1kHz sine wave
E causes malfunctions when its noise exceeds 0dBm at 7kHz (its most susceptible frequency) or +20dBm at 1kHz

Figure 3 Example with two susceptible frequencies

Some test standards (especially military) use 1kHz square

A simplified and earlier version of this paper (6 pages) was published in the Proceedings of the IEEE International EMC Symposium, Austin, TX, August 17-21, 2009, ISBN (CD-ROM): 978-1-4244-4285-0.

wave modulation instead of sine. The advantage is that the spectrum of a square wave has components at all of the odd-order harmonics (3rd, 5th, 7th, etc.), and so tests with many modulation frequencies at once. The amplitudes of the harmonic components diminish in amplitude as their harmonic order increases, according to the usual Fourier series.

Square wave modulation at 1kHz contains a 7kHz component at a level of about 17dB below the level of the 1kHz component. For this 7kHz component to reach 0dBm in E, and cause interference, the level of the 1kHz component causing noise in both D and E would be 17dBm, so once again D would fail first, hiding the potential failure of E in real life, or causing it to be misjudged.

So testing with a simple modulation cannot predict real-life behavior in the electromagnetic environment, a conclusion that is also reached by [32] and [33].

Rectification and intermodulation

The electrical noise that causes the errors or malfunctions that we call EMI can arise due to three quite different mechanisms:

- From unmodulated ‘carrier’ frequencies, which is often called ‘direct interference’
- From new frequencies generated by the rectification in the non-linearities inherent in semiconductor devices (and corroded electrical contacts). These occur as baseband noise (amplitude modulated DC offsets), that is the envelope of the carrier frequency (or the sum, where there is more than one), and as harmonics of all of the carrier frequencies (2nd, 3rd, etc.).
- From the intermodulation of two or more frequencies present simultaneously, whether they are noises or wanted signals, again caused by the non-linearities as above.

Figure 4 shows a very simple example of all three mechanisms. The example 400MHz (*f1*) and 500MHz (*f2*) noises in the circuit are caused by its EM environment. Rectification causes baseband noise that is the sum of both of the modulations of the two original noises, plus a wide range of harmonics, of which only the 2nds fit on Figure 4. Intermodulation between f1 and f2, and between those original frequencies and their harmonics, gives rise to further new frequencies in the circuit at their various sums and differences, some of which are shown in Figure 4.

In real EM environments, the number of frequencies present at significant levels is not limited to two, and so the number of new frequencies arising due to rectification and intermodulation can be very large. The chances of a new noise frequency landing on an especially susceptible frequency is greater than that of the original frequencies that created them.

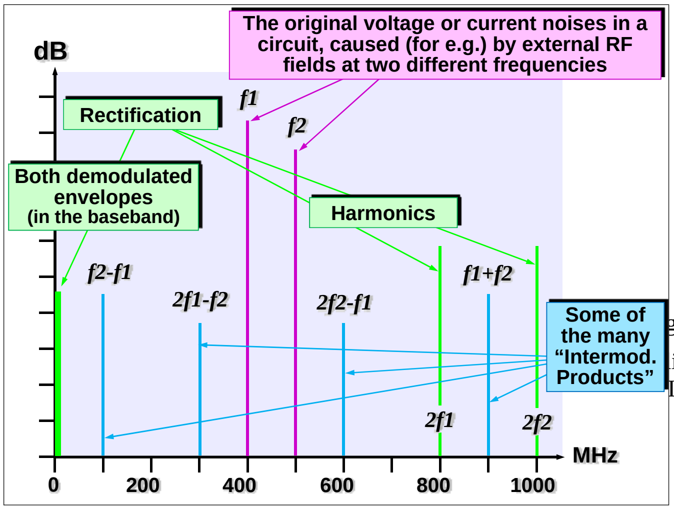
The original voltage or current noises in a circuit, caused (for e.g.) by external RF fields at two different frequencies
dB
Rectification
f1
f2
Both demodulated envelopes (in the baseband)
Harmonics
f2-f1
2f1-f2
2f2-f1
f1+f2
Some of the many “Intermod. Products”
2f1
2f2
MHz
0
200
400
600
800
1000

Figure 4 Simple example of noises coupled into a circuit

Almost without exception, standardized immunity tests for continuous disturbances use a single carrier frequency, with one modulation frequency (or a limited range of them). EMC engineers have become adept at solving immunity problems caused by such tests, but it is possible for two or more frequencies that – by themselves – caused no interference when tested, to rectify and intermodulate and cause interference when they are present at the same time. [32] also makes this point.

For example, assume that the single-frequency immunity tests spanned 10MHz to 10GHz, but only caused interference over 10 to 500MHz in a given item of equipment. EMC engineers added shielding and filtering that was effective over that frequency range and made the equipment pass the tests over the whole range. This scenario is repeated hundreds of times daily in test laboratories around the world.

But in real EM environments, two or more frequencies outside the range of effectiveness of the 10-500MHz shielding and filtering are still allowed to enter the circuit. These frequencies cause no problems *in themselves*, but will rectify and intermodulate in the circuits to produce new frequencies that could fall within the susceptible range of 10 to 500MHz, causing interference.

It does not matter what levels the original tests were carried out at, they cannot simulate the real-life effect of multiple frequencies.

Physical stresses, ageing, corrosion, wear, faults, misuse, etc.

Over its lifecycle, equipment will be exposed to a wide range of physical and climatic conditions, such as: mechanical stresses, shocks and vibration; humidity, moisture, liquids and gasses causing corrosion; temperature and air pressure variations; dusts, mould growth, etc. It will also suffer from wear due to repetitive mechanical functions and operator actions.

These can all degrade EM mitigation measures, increasing susceptibility to EM disturbances. For example filters can suffer degraded ground bonds, and shielding can suffer degraded joints and gaskets. Surge protection devices and suppression capacitors will wear out and fail when exposed to a sufficient number of surges of sufficient amplitude.

These influences can also directly affect the EM ‘hardness’ of the circuits themselves, increasing their susceptibility.

Faults, arising during assembly, installation or operation, can also increase susceptibility by degrading an equipment’s EM characteristics in similar ways to those discussed above, as can poor installation, misuse during operation, or failure to perform certain maintenance tasks correctly.

But applying immunity tests at increased levels can almost never address these concerns *in practice*, and so cannot help achieve confidence in real-life reliability over the lifecycle.

ished in the Proceedings of the IEEE International EMC Symposium,
ISBN (CD-ROM): 978-1-4244-4285-0.

For example, if an equipment relies upon a 60dB shielding enclosure, but is not suitable for its physical/climatic environment so eventually the gaskets around its access door corrode and cease to make good electrical bonds – or if the operator simply leaves the door open – then it would be necessary to test with an additional margin of 60dB, for example increasing the test level from 10V/m to 10kV/m. Similar arguments apply to testing for degraded filters.

Of course, one could simply repeat the normal EM immunity test program with all of the possible instances of physical stresses, ageing, corrosion, wear, faults, misuse, etc., applying appropriate margins to the test levels. The test plan would become very much longer, and the cost of the test equipment very much higher, but it might nevertheless be possible.

However, since mechanical stresses, shocks, vibration, ageing, corrosion, wear, faults, misuse, etc. are all independent variables, they can occur in a very wide range of reasonably foreseeable combinations. EM immunity testing with just one phenomenon simulated, at any test level, cannot cover the effects of reasonably foreseeable *multiple* phenomena.

So although is *theoretically possible* to perform EM immunity tests that would deal with all of these foreseeable phenomena – it is *almost never practical* to do so, due to the absolutely huge timescales (hence costs) that would be required.

The above has shown that applying the normal immunity tests to a perfectly constructed fault-free brand-new item of equipment, operated in accordance with its User Manual, only covers a small fraction of the possibilities for EMI to cause problems in real life, over the whole lifecycle.

It has also shown that increasing immunity test levels, even by large margins, cannot significantly increase the test coverage and achieve sufficient confidence where electronic devices must operate with high reliability.

Several more issues

The above discussed a few of the major reasons why simply applying the normal EM immunity tests at higher levels cannot provide sufficient confidence that high levels of reliability will be achieved in real-life applications, over the lifecycle.

It focused mainly on testing with continuous radiated or conducted EM disturbances, but similar shortcomings arise with transient disturbance immunity testing, see [19].

There are several more shortcomings in the use of the normal immunity test methods – even if they use increased test margins – for demonstrating high-reliability despite EM disturbances. Lack of space prevents them being discussed here, but they are discussed in [14] [20] [21] [22] and [23].

III. WHAT SHOULD BE DONE (VERY BRIEFLY)

One consequence of the above, discussed in more detail in [1] [14] [20] [21] [24] and [25], is that the number of issues that could have a negative impact on equipment reliability, make it impossible to create an EMC test plan that could cover them all. So other techniques must be used to demonstrate the achievement of the desired reliability.

This is a similar situation to that facing the safety-related software industry in the 1990s – which, after great efforts in academia and industry, resulted in the creation of a range of software engineering techniques, and a range of verification and validation methods, now well-established and described in IEC 61508-3 [26].

However, the work on similar EMC engineering techniques and verification and validation methods has only just begun, see [1] [14] [27] and [28]. Although these references are concerned with safety systems, their approaches are equally relevant for high-reliability and mission-critical equipment – except that “fail-safe” design may not be appropriate.

Appropriate verification and validation methods for EM immunity include (but are not limited to):

a) Demonstrations. Such as demonstrating that the reliability requirements have been correctly implemented.

b) Checklists. For example, to ensure that EMC design measures have been observed, applied and implemented correctly.

c) Inspections. For example, checking that the assembly and installation have followed the EMC requirements correctly.

d) Reviews and Assessments. These ensure compliance with the objectives of each phase of the lifecycle. Usually performed by experts.

e) Audits. Including checking that correct specification, design, assembly, installation, verification and validation processes have been followed.

f) Non-standardized checks and tests. There are very many non-standard EMC checks and tests that can (and often should) be developed to improve confidence in lifecycle reliability, often without adding significant delays or costs.

g) Individual and/or integrated hardware tests. Different parts of the equipment are assembled step-by-step, with appropriate checks and tests applied at each step. Most appropriate for large systems or installations.

h) Validated computer modeling. Computer-aided EMC design is now routinely used in some critical applications ([29]) to reliably reduce design and test timescales.

All computer modeling is based on simplifications, so it is important to validate any predictions by appropriate testing. But once the model replicates the test results with sufficient fidelity, it can be used to very quickly simulate the results of many similar tests that would be too costly or time-consuming to perform in real life.

i) Testing (e.g. factory acceptance test or on-site testing). Although EM immunity testing can never be *sufficient* for demonstrating high reliability, it is still an important verification and validation method. However, the testing methods used may need to be modified to improve test coverage to achieve confidence for reliability issues that have not been able to be adequately addressed by other methods.

In some cases it will be appropriate to use the ‘normal’ test methods, modified a little (e.g. by using different modulation frequencies or types, or increasing the duration of transient tests to cover more of the possible software states). In other cases it will be necessary to create unique non-standardized tests, maybe even using close-field probing. The project documentation should justify all modified or new test methods, to a degree commensurate with the level of reliability required, or the criticality of the equipment's function.

A philosophical point

A common response from many EMC test professional when faced with the arguments that have been presented in this paper, is to say words to the effect that: "There is no evidence that EMI has contributed to safety incidents, therefore the EMC testing we do at the moment is sufficient for safety".

But the assumption that because there is no evidence of a problem, therefore there is no problem, was shown to be logically incorrect in the 19th Century (by William Cowper) and (to give just one example) its use by NASA management led directly to the Columbia space shuttle disaster [34].

Anyone who uses such an argument for there being no need to do much more than increase testing levels a little, if anything, is either very poorly educated themselves, or assumes that their audience is.

If engineering risk analysis shows that something can be interfered with and cause a safety incident, it will happen at some time. If the risk of it happening is higher than the agreed tolerable risk level, it must be reduced until it is tolerable.

IEC 61508 [4] compliance requires a demonstrated engineering confidence that the mean time to dangerous failure of a safety system is between 10 years (minimum, SIL1) and 10,000 years (minimum, SIL4).

It is likely that safety incidents caused by EMI will not be identified as being caused by EMI, because they occur so infrequently, because EMI often leaves no trace of its occurrence after an incident, and also because of the well-known difficulties of determining what EMI could have caused the incident (all of these being difficulties that help support erroneous "There is no evidence…..therefore…." claims mentioned above).

But a lack of evidence does not exempt us as engineers from having to reduce the probability of safety incidents due to EMI to agreed tolerable risk levels.

CONCLUSIONS

It has been shown that EM immunity testing – with test levels increased by whatever margins – *cannot be sufficient* to demonstrate that high-reliability, mission-critical or safety-critical equipment will achieve its reliability (or safety risk) specifications despite the EM disturbances over its lifecycle.

Appropriate design engineering, and a range of verification and validation methods are required for such applications. These have been briefly discussed and references will aid further study.

EMC testing professionals have been used to EMC validation methods being objective and repeatable, giving the same results when tested by different people in different test laboratories anywhere in the world. Well, this sounds like a nice goal (although it is still some way from being achieved with errors that look tolerable when expressed in percentages, rather than dB!) – but the problem with trying to achieve the parts-per-million reliability levels (or less) that are required for the higher SILs (see [4]) is that *affordable* testing can only take us part of the way. All the other engineering disciplines (e.g. software) have learned to use subjective risk-assessment based techniques such as those described in IEC 61508 [4], to take the reliability the rest of the way.

No doubt, subjective verification/validation techniques for EMC design will take some time to percolate through the EMC community and become established – just as subjective techniques are even now penetrating the software engineering community.

But EMC immunity testing alone cannot achieve the confidence we need for functional safety, no matter how high test levels are increased.

REFERENCES

[1] IEC/ TS 61000-1-2, Ed.2.0, 2008-11, basic safety publication, "Electromagnetic Compatibility (EMC) – Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena", http://webstore.iec.ch.

[2] Moore's Law, see http://en.wikipedia.org/wiki/Moore's_law

[3] "The First 500 Banana Skins", Nutwood UK, Oct. 2007, a compendium of anecdotes, reports, etc., on EMI incidents, from http://www.emcacademy.org/books.asp.

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

[5] MIL-STD-464, "Electromagnetic Environmental Effects – Requirements for Systems", Department of Defense Interface Standard, March 18 1997.

[6] RTCA/DO-160F, December 6, 2007, "Environmental Conditions & Test Procedures for Airborne Equipment", Section 20, Radio Frequency Susceptibility (Radiated and Conducted)". Also recognized as de facto international standard ISO-7137.

[7] IEC 60601-1-2 Ed. 3.0 March 2007, "Medical Electrical Equipment – Part 1-2: General requirements for basic safety and essential performance – Collateral standard: Electromagnetic compatibility – Requirements and tests", http://webstore.iec.ch.

[8] Most of the IEC 61000-4 standards, http://webstore.iec.ch.

[9] Telcordia GR-1089-CORE "Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunication Equipment"

[10] A number of ITU Engineering Recommendations in the ITU-T 'K' series, http://www.itu.int.

[11] All major automobile manufacturers have in-house EMC immunity test requirements, for example: BMW Group Standard GS 95002, 2004-10, "Electromagnetic Compatibility (EMC) — Requirements and tests".

[12] ISO 7637-2:2004, "Road vehicles -- Electrical disturbances from conduction and coupling -- Part 2: Electrical transient conduction along supply lines only".

[13] ISO 11451 "Road vehicles – Vehicle test methods for electrical disturbances from narrowband radiated electromagnetic energy". Part 1, "General principles and terminology"; Part 2,

"Off-vehicle radiation sources"; Part 3, "On-board transmitter simulation"; Part 4, "Bulk current injection (BCI)".

[14] "EMC for Functional Safety", the IET's practical guide, August 2008, free download from www.theiet.org/factfiles/emc/index.cfm, or purchase as color-printed book from http://www.emcacademy.org/books.asp.

[15] "Assessing an EM Environment", Technical Guidance Note No. 47, EMC Test Labs Association (EMCTLA), www.emctla.co.uk/Pages/TechGuideMain_new.html

[16] Keith Armstrong, "Specifying Lifetime Electromagnetic and Physical Environments – to Help Design and Test for EMC for Functional Safety", 2005 IEEE Int'l EMC Symposium, Chicago, 8-12 Aug., ISBN: 0-7803-9380-5, pp 495-499.

[17] CISPR 16-4-2, "Specification for radio disturbance and immunity measuring apparatus and methods - Part 4-2: Uncertainties, statistics and limit modelling - Uncertainty in EMC measurements"

[18] Zulfiqar Ali Khan, Charles F. Bunting and Manohar D. Deshpande, "Shielding Effectiveness of Metallic Enclosures at Oblique and Arbitrary Polarizations", IEEE Trans. EMC, Vol. 47, No. 1, February 2005, pp 112-122.

[19] Y. Bayram *et al*, "High Power EMI on Digital Structures Within Automotive Structures", 2006 IEEE Int. EMC Symp., Portland, 14-18 Aug., ISBN: 1-4244-0924-8

[20] Keith Armstrong, "Why EMC Immunity Testing is Inadequate for Functional Safety", 2004 IEEE Int'l EMC Symp., Santa Clara, Aug. 9-13 2004, ISBN 0-7803-8443-1, pp 145-149. Also: Conformity, March 2005, http://www.conformity.com/artman/publish/printer_227.shtml.

[21] Keith Armstrong, "Functional Safety Requires Much More Than EMC Testing", EMC-Europe 2004 (6th International Symposium on EMC), Eindhoven, The Netherlands, 6-10 Sept., ISBN: 90-6144-990-1, pp 348-353.

[22] Keith Armstrong: "EMC in Safety Cases — Why EMC Testing is Never Enough", EMC-UK 2007 Conference, Newbury, UK, Defence & Avionics session, 17 Oct.

[23] Keith Armstrong: "EMC for the Functional Safety of Automobiles — Why EMC Testing is Insufficient, and What is Necessary", 2008 IEEE Int'l EMC Symp., Detroit, 18-22 Aug., ISBN 978-1-4244-1699-8 (CD-ROM).

[24] D A Townsend *et al*, "Breaking All the Rules: Challenging the Engineering and Regulatory Precepts of Electromagnetic Compatibility", 1995 IEEE Int. EMC Symp., Atlanta, pp 194 – 199.

[25] Keith Armstrong, "The IET's New Guide: EMC for Functional Safety – Applying Risk Management to EMC", The EMC Journal, November 2008, pp 27-34, www.theemcjournal.com

[26] IEC 61508-3: "Functional Safety of Electronic/Electronic/Programmable Electronic Safety-Related Systems – Part 3: Software Requirements".

[27] Keith Armstrong, "Design and Mitigation Techniques for EMC for Functional Safety", 2006 IEEE Int. EMC Symp., Portland, 14-18 Aug., ISBN: 1-4244-0294-8.

[28] K. Armstrong, "Validation, Verification and Immunity Testing Techniques for EMC for Functional Safety", 2007 IEEE Int. EMC Symp., 9-13 July, Honolulu, ISBN: 1-4244-1350-8.

[29] Ian MacDiarmid of BAE Systems, presentation to the EMCIA, London, UK, 14 Dec. 2006, www.emcia.org.

[30] Qi-Feng Liu, Wen-Yan Yin, Ming-Feng Xue, Jun-Fa Mao and Qing-Ho Liu, "Shielding Characterization of Metallic Enclosures With Multiple Slots and A Thin-Wire Antenna Loaded: Multiple Oblique EMC Incidences With Arbitrary Polarizations", IEEE Trans. EMC, Vol. 51, No. 2, May 2009, pp 284-291

[31] C A Grosvenor, D Novotny, D Camell, G Koepke, R Jonk and N Canales, "Electromagnetic Penetration Studies for Three Different Aircraft", IEEE International EMC Symposium, Austin, TX, August 17-21, ISBN: 978-1-4244-4285-0

[32] Ron Brewer, "EMC Failures Happen", Evaluation Engineering, December 2007, http://www.evaluationengineering.com/features/2007_december/1207_emc_test.aspx

[33] I. D. Flintoft, "Preliminary Investigation Into a Methodology for Assessing The Direct RF Susceptibility of Digital Hardware Final Report for Radiocommunications Agency", Document number R/99/042, Project number 0921, York EMC Services Ltd, 12th May 1999, www.ofcom.org.uk/static/archive/ra/topics/research/topics/emc/r99042/r99042.pdf

[34] Keith Armstrong, "Absence of proof is not proof of absence (and the 'proven in use' fallacy)", The EMC Journal, Issue 78, Sept 2008, pp 16-19, www.theemcjournal.com