Another EMC resource
from EMC Standards

Functional safety requires much more than EMC testing

Helping you solve your EMC problems

9 Bracken View, Brocton, Stafford ST17 0TF T:+44 (0) 1785 660247 E:info@emcstandards.co.uk

FUNCTIONAL SAFETY REQUIRES MUCH MORE THAN EMC TESTING

EurIng Keith Armstrong
Cherry Clough Consultants
Cherry Clough House, Rochdale Road, Denshaw, OL3 5UE, Great Britain
E-mail: keith.armstrong@cherryclough.com

1. ABSTRACT

Electronic and programmable electronic devices are increasingly being used to control appliances, equipment, vehicles and systems where errors or malfunctions in those devices can have functional safety implications. All such devices can suffer from electromagnetic interference (EMI).

The functional safety of such equipment is covered by IEC 61508 [1] – but their EMI requirements are not (yet) correctly specified by any safety or electromagnetic compatibility (EMC) standards.

This paper lists the shortcomings in existing EMI provisions, then introduces techniques for ensuring that EMI does not cause functional safety problems.

2. INTRODUCTION

Electronic devices (especially software programmable electronic devices) are increasingly being used in safety-implicated, safety-related and safety-critical applications, especially in industrial, commercial, medical, transportation, military vehicles and weapons. The reliable performance of these electronic devices is often of concern for functional safety.

All electronic devices can suffer inaccuracy, malfunction, even permanent damage when exposed to the electromagnetic (EM) disturbances in their operating environments.

The continued shrinking in the feature sizes of electronic devices adds to their functionality and reduces their cost – but this shrinking, and its associated lower operating voltages, makes the devices more susceptible to EMI. Combined with the fact that EM environments are continually worsening, due to the increasing use of modern electronic devices, the resulting decreasing reliability has serious consequences for functional safety.

Functional safety problems can concern appliances, equipment, vehicles, systems and installations (however large) – all of these are covered by the word 'equipment' in the remainder of this paper.

EMC standards and regulations (such as the European EMC Directive, 889/336/EEC, amended) generally do not address functional safety, whilst safety standards and regulations generally deal with EMI related issues very poorly, if at all [2], [3]. The resulting lack of coverage of this increasingly important safety issue [2] leaves manufacturers without official guidance. Most manufacturers only comply with minimum regulatory requirements, so functional safety risks are increasing, as shown by Figure 1.

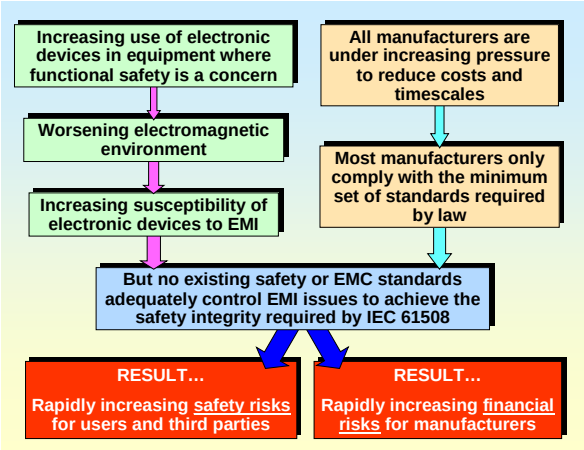

Fig. 1 – Increasing functional safety risks from EMI

The IEE (London, UK) published a guide on this issue in 2000 [2], employing an approach based on 'EMI hazards analysis and risk assessment'. In 2004 the IEE began to run a series of training courses [4].

Of all the EMC standards publicly available (including automotive manufacturer's in-house standards) and known to the author, only MIL-STD-464 [5] and IEC/TS 61000-1-2 [6] employ a suitable approach.

[5] is most suitable for military and aerospace equipment, but can be modified to apply to other areas. [6] is a 'Technical Specification' and not (yet) a full IEC standard. They both employ hazard analysis and risk assessment approaches similar to the IEE's 2000 guide.

IEC product safety committees have recently begun to add EMI requirements for functional safety to their standards. But instead of following the hazards and risk based approaches of [5] and [6] they are simply adding immunity test requirements like those used for EMCD compliance [7]. These types of tests are called 'normal' immunity tests in the rest of this paper.

Unfortunately, as this paper will show, normal immunity testing is inadequate as the sole means of demonstrating that an acceptable level of EM performance has been achieved for functional safety.

Safety performance is generally verified by…

- Inspecting the design against a number of safety

design criteria well-proven to provide a sufficient level of lifecycle protection, including the effects of the physical environment and foreseeable use
- Fault testing samples of the finished design
- Basic safety checks on every item manufactured

But normal immunity testing simply tests one or two new samples of the finished equipment in a benign physical environment. This approach is quite different from that taken for all other safety issues, including software [8], and it is not adequate for functional safety purposes, as the next section will show.

3. SHORTCOMINGS IN NORMAL IMMUNITY TESTS

3.1 Faults are not addressed

Faults arising in components, or during assembly, delivery, operation, maintenance or repair can significantly affect an equipment's immunity to its everyday EM environment. For example…

- Dry joints or short circuits (e.g. in a filter)
- Incorrect / out-of-tolerance electronic components
- Incorrect, loose or missing fixings associated with shielding or radio-frequency bonding
- Damaged or missing conductive gaskets
- Failure of a surge protection device

Safety standards simulate foreseeable faults to check that the equipment remains safe, but normal immunity tests only use perfect equipment. In the author's view, this shortcoming alone shows that normal immunity testing is inadequate as a means of proving that EMI will not increase functional safety risks.

3.2 Real EM environments not simulated

Real life exposes equipment to a number of *simultaneous* EM disturbances, for example: radiated fields from two or more radio channels; a radiated field plus an electrostatic discharge; etc. Measurements by Michel Mardiguian show that during one EM disturbance, an equipment's immunity to another disturbance can be significantly reduced [9].

The waveforms used for transient immunity tests are very simple compared with the multitude of real disturbances they simulate. But the susceptibility of circuits and the effectiveness (and lifetimes) of suppression devices depend strongly on voltage and current waveforms.

Modulating an interfering signal at the rate of the digital signals in an equipment can significantly reduce its immunity [10], [11]. But although EM environments can include a huge range of modulations, normal immunity tests simply use 1kHz sine-wave (and 0.5Hz for some medical devices).

Normal radiated EM field immunity compliance testing employs anechoic chambers that are unlike most real-life EM environments. In many real applications there are nearby surfaces reflecting EM fields from a variety of angles. If the layout of the equipment and related cables in an anechoic chamber test is not identical to its set-up in real life (it usually is not), the test results can differ from the equipment's real-life radiated susceptibility. Also, there are concerns about the uncertainty in the anechoic chamber test method itself, with some authors suggesting large and unpredictable uncertainties [12], [13]. Tests that use reverberation chambers can be better in these respects [14], [15].

3.3 EMI 'risk assessment ' not done

Normal immunity tests do not cover the close proximity of cellphones, although this is now commonplace and can expose equipment to much higher radio-frequency fields and/or frequencies than the normal tests. Normal tests also only apply transients of up to ±2kV on the AC power supply, although it has long been established that ±6kV can occur on typical single-phase supplies [16]. Other failures to cover the typical modern EM environment could be listed.

Normal immunity tests make no attempt to cover low-probability EM disturbances, even though they can be very important for functional safety (especially where safety integrity requirements are high, see [1]).

Simon Brown and Bill Radasky said [17]: *"Generic EMC standards have been developed to advise product committees on the "essential" immunity tests and their levels depending on the location of the equipment (home, industry, power substations, etc.). The problem is that some of the EM environments not considered "essential" for EMC could produce a safety hazard in some systems."*.

Some safety test standards (such as the latest edition of the medical device safety standard EN 60601-1-2) increase the tested frequency range or test levels (doubling the test levels is a particular favourite). But simply 'toughening' the normal immunity tests is no substitute for a proper "EMI risks assessment".

3.4 "Compatibility Levels" too relaxed

The question arises of where to set the pass/fail level for an immunity test, within the statistical variation of the foreseeable EM environment. This is known as the "Compatibility Level", and it is often set at the two-sigma point (sigma being the standard deviation) – meaning that 95% of the events of a given type of EM disturbance will fall below the tested level. But 5% of the disturbances will exceed the tested level.

Two-sigma compatibility might be a good general compromise between performance and cost, but could be unacceptable where there are functional safety implications – especially where safety integrity requirements are high.

3.5 Physical environment not considered

To achieve functional safety over an equipment's lifecycle, suitable EM performance must be maintained despite the effects of the physical environment. These effects can be immediate, or long-term (ageing).

Immediate effects include those caused by extremes of temperature and supply voltage, shock, vibration,

loading, condensation, icing, physical forces, etc., operating on the enclosure. [18] describes measurements that show how the supply filter of a variable speed motor drive can have up to 20dB worse performance than measured by normal EMC tests, under easily foreseeable circumstances.

Other immediate effects include causing faults such as poor contact at radio-frequency bonds and conductive gaskets; short-circuits; and a variety of other effects that can reduce the effectiveness of filtering, shielding or suppression and make equipment less immune.

An equipment's lifecycle exposure to its physical environment, including condensation, liquid spills and spray, mould growth, sand, dust, cleaning (e.g. wire-brushing, solvents) and repainting – plus wear and tear caused by multiple operations of controls and the opening and closing of doors and access panels, temperature cycling, etc. – all contribute to 'ageing'. Ageing always degrades EM performance. One effect of ageing is corrosion at metal joints, a well-known and inevitable effect known to degrade EM filtering and shielding performance with time.

But although functional safety should be maintained over the life of an equipment, normal immunity tests are only applied to pristine new samples, in a benign environment, and never address the immediate or ageing effects of the physical environment.

[19] concludes: *"Commercial or military EMC testing is seldom combined with climatic or dynamic (vibration and shock) testing. The authors decry this lack. This article encourages a comprehensive approach approximating actual in-service conditions. RF Test (Audio Frequency Conducted Susceptibility – Power Inputs Test, Radio Frequency Susceptibility Test, Induced Signal Susceptibility Test, Emissions of Radio Frequency Energy Test) should be combined with climatic (temperature, altitude, humidity, waterproofness testing, fluid susceptibility testing, sand and dust testing, fungus resistance testing, salt spray testing) and with dynamic (sawtooth mechanical shock, sine and random vibration, explosion proof) tests."*

3.6 Only a representative sample is tested

Most manufacturers design, test using normal immunity test methods, then modify – iterating until their new equipment passes the tests. But most of them have no idea whether the final version passed because of good design, or because of something that might not be adequately controlled in future manufacture.

For example, semiconductor suppliers will supply 'die-shrunk' devices – indistinguishable (visibly and operationally) to previously supplied types – without warning. These can have a marked effect on the EMI performance of the equipment.

Many companies introduce 'small' changes in production (e.g. altered cable routes; modified fixing methods; software 'bug fixes'; substitute components; etc.,) – without re-measuring immunity. Many do not routinely test EMI performance in serial manufacture either, so they cannot know the actual EMI performance of the equipment they supply.

Even if a sample once passed an immunity test, on its own this proves nothing at all about the immunity performance of the equipment actually supplied.

3.7 Maintenance, repair, refurbishment, upgrades

In real life, equipment is subject to cleaning, maintenance, repair, refurbishment and upgrades. Safety test standards take some of these issues into account as a matter of good safety engineering practice – but normal immunity testing does not.

3.8 Performance degradations

It can be difficult to test the immunity of a system, so tests on individual items or sub-assemblies are often considered adequate instead. But a simple example will show that this can lead to problems.

Normal immunity testing permits a DC power supply to meet Performance Criterion B during a FTB test (using IEC 61000-4-4) – which means that any amount of momentary degradation is permitted during the test as long as the equipment self-recovers immediately afterwards. Protection circuits in some power supplies cause their outputs to collapse to 0V during each fast transient burst, but this is considered acceptable.

But where such a DC power supply powered a microprocessor, collapsing its DC rail to 0V would cause it to reboot. Afterwards, the equipment might not be in the same operational state as was required for functional safety. Even if rebooting restored the original operation, correct functionality would not be available during rebooting and this could be important for some types of safety functions.

This example shows that EMC testing individual items of equipment does not necessarily mean that their immunity performance will be acceptable when they are used in a safety-implicated system.

[17] suggests: *"All performance degradations observed in immunity testing should be documented and reported in the equipment documentation. Performance degradations should be evaluated from the viewpoint of safety. Testing should be performed at the highest practical level of integration."*

4. CORRECTLY DEALING WITH EMC FOR FUNCTIONAL SAFETY

4.1 Overview of the approach

The correct method of dealing with EMC for Functional Safety is to follow the usual safety engineering approach, based on a hazards and risks assessment:

- Determining what stresses (EM and physical) the new equipment will foreseeably be subjected to
- Deciding a functional safety performance specification that takes into account the safety integrity required (see [1])

- Designing to achieve the specification despite the application of the stresses over the whole lifecycle
- Verifying the design
- Ensuring that manufacture, maintenance, repair, refurbishment and upgrades don't reduce the functional safety performance below specification

EMC testing has a number of important parts to play in all parts of the above process. But the test methods that are used might differ from normal immunity tests.

4.2 Assessing the EM environment

The reasonably foreseeable EM stresses (sometimes called threats) that the equipment could be subjected to should be assessed and quantified. A statistical analysis of the occurrence of each EM threat will help decide the equipment's EM specification. However, some safety integrity requirements could require even very low probability threats to be coped with.

Published information on the EM environment is fragmented, and is usually specific to particular areas. For instance, a great deal of statistical information exists on threats from lightning, and on (or in) military vehicles such as aircraft and ships. The IEC 61000-2 series of standards also provides valuable information on certain aspects of the EM environment.

Comprehensive EM environment information on other areas (e.g. rail, road, hospitals, etc.) may be harder to find, and may be proprietary to certain organisations. Instrumented site surveys can be performed, but measuring low-probability disturbances can require very long measuring times.

An assessment of an EM environment should cover the areas shown in Figure 2.

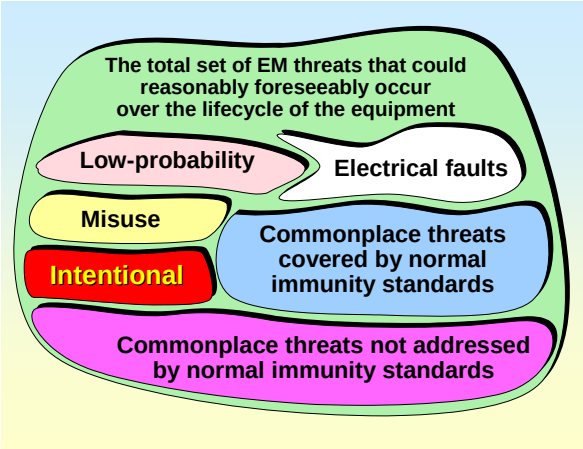

Figure 2 – Foreseeable EM threats

It is important to understand that 'compatibility levels' (or 'test levels') specified by standards will not have taken into account the safety integrity requirements of the new equipment. The statistical distribution of each EM threat is required to decide the specifications for the new equipment. Where such information does not exist, expert threat assessments are required.

It is increasingly important to consider intentional EM threats [20]. These might arise from competitors, disgruntled employees, terrorists, criminals, or others.

Where an existing design of equipment is to be sold into an environment not considered during its original design, an assessment of the new threats is required that could lead to design changes and reverification.

4.3 Assessing the physical environment

There are well-known IEC and military standards that describe the physical and climatic characteristics of a wide variety of environments, including storage, transport and operation. As for the EM environment, the statistical distribution of each physical threat is required, and any 'compatibility levels' (or 'test levels') they specify should be treated with great caution.

Each new design should also consider reasonably foreseeable use and misuse, such as failing to follow the user instructions. 'Brainstorming' techniques using a wide variety of participants are often required to do this effectively.

4.4 Safety integrity requirements

[1] includes methods for establishing the safety integrity requirements for complete safety-related systems, and for the items of equipment which are used in those systems. It also includes a number of design requirements that are related to the required safety integrity, such as double or triple redundancy. Software, like EMC, cannot sensibly rely solely on testing to prove that it is safe enough, so [8] specifies the software design methods that should be used for compliance. [1] lacks a similar section on EMC design techniques, but maybe [6] will be developed to fill this requirement.

4.5 Equipment specifications

Once the EM and physical environments have been assessed and safety integrity requirements determined for the application, appropriate EM and physical performance specifications can be written to guide the design and verification processes.

These will specify the permissible degradation in each relevant functional performance issue, *when* the equipment is subjected to reasonably foreseeable combinations of both EM and physical threats for its complete lifecycle.

4.6 EM design techniques

There are a great many publications on the EMC design techniques that can be applied at different levels of assembly (integrated circuit; circuit; printed circuit board (PCB); interconnection; shielding, filtering and suppression of PCBs, modules, sub-assemblies, enclosures, rooms and buildings; etc.).

It is often more cost-effective to employ a number of different 'layers' of EM mitigation instead of relying on just one layer (such as enclosure and cable shielding). Using multiple layers of mitigation also helps deal with foreseeable faults and even unforeseen problems.

A technique used by some is to inject a variety of signals into circuits that have had any filtering,

shielding or other suppression removed, to determine their 'natural susceptibilities'. The results are then analysed to see how those natural susceptibilities might possibly be influenced by the EM environment, to help select EM mitigation techniques.

The EM performance required for functional safety should be maintained over the equipment's lifecycle (and lifetime). So, for example, when designing a conductive gasket for a door in a shielded enclosure, the designer should consider that the door will be subjected to bending and twisting from non-ideal installation (such as a non-flat floor or wall, or other equipment stacked on top) and temperature extremes.

He/she should also consider the long-term effect on the gasket's EM performance of opening and closing the door hundreds (thousands?) of times over its life; plus the effects of corrosion, mould growth, sand, dust, grease, vibration, etc.

Highly-accelerated life testing ('HALT') is a powerful tool for assessing the suitability of design methods such as the gasketting mentioned above. Equipment for safety-related applications will often be HALT tested anyway, so all that may be required is adding some EMC tests (e.g. shielding effectiveness) during or after the HALT tests.

As soon as one mentions combining EMC and HALT tests most EMC test engineers immediately say that they cannot place shock, vibration, or climatic test facilities in their anechoic chambers. But it is *relative* EM performance we are interested in, not *absolute* measurements. It can be very easy and inexpensive to instrument a HALT test to detect degraded EM performance during or after a test, but the test methods will have to be uniquely designed. All EMC tests should relate to the foreseeable EM environment, for example in frequency range or waveshape.

Other EMC tests may need to be devised to verify the suitability of a particular design technique for meeting the lifecycle EMC and physical specifications. Some design methods might be verified by calculation or simulation, and some by previous experience with other equipment in related environments.

4.7 Verifying equipment EM performance

The unsuitability of normal EMC test methods was discussed earlier, to show that they could not be relied upon as the *sole means* of proving EM performance where functional safety was an issue.

By following a correct approach as briefly discussed above, a good design team should be able to prove that there is no need to perform any EM tests on the finished equipment (and their design documentation should show this). But final design verification tests *are* required. Since the normal immunity test methods may not always give sufficient confidence – the testing to be applied should be carefully designed to discover whether the equipment could suffer from any 'EM weaknesses' in its real environment.

For example, military and aviation experts have recently developed a method for testing aircraft flight controls, weapons, and other safety-related equipment for immunity to radiated radio-frequency fields.

This method uses a reverberation (mode-stirred) chamber because its results can be correlated with the reflectivity of the application's intended EM environment. Reverberation chambers can cost a great deal less to construct and equip than the anechoic chambers used for normal testing, and they can be made very large indeed.

The reverberation chamber's 'stirrer' is rotated over a full revolution, in a series of steps (usually between 20 and 120). At each step, radio frequency fields are generated in the chamber by a signal generator power amplifier, and antenna. These fields are appropriate in frequency range and magnitude for the foreseeable radiated threats in the operational EM environment.

At each stirrer step, the whole frequency range is covered in small steps (sometimes as low as 0.1%) – and at each frequency step the radio field is 'chirp modulated' over the range for which the equipment has foreseeable susceptibility (e.g. 30Hz - 30kHz) and also switched off and then on again.

The time taken to complete a single 'chirp + off/on' depends on the response time of the safety function being tested. If necessary, time can be saved by monitoring critical electronic points within the equipment with special high-immunity probes.

4.8 Quality control (QC)

A design is no good unless the QC in manufacturing ensures the correct build-state. Problems with EM performance can arise due to: variations in purchased parts; alternative or replacement parts; variations in plating, painting and fixing; differences in assembly; design changes and improvements, 'bug-fixes' and upgrades; etc. Similar issues apply to manufacturing done by subcontractors.

All of the build-state issues relevant for EM performance should be identified during the design process and controlled by QC in manufacturing. QC can use a range of techniques, including 'EM checks' on delivered parts, PCBs, modules, sub-assemblies, and finished equipment. They should also use 'work instructions', visual inspections, and change control.

EM checks are relative tests, designed to detect differences from the ideal build-state. They can be surprisingly easy to set up and can de designed to require very little expertise to operate.

QC should employ competent personnel, backed up by appropriate testing, to assess every design change proposal for its EMC and functional safety implications.

4.9 Maintenance, repair, refurbishment, upgrades

Just as in manufacturing, QC techniques are required in maintenance, repair, refurbishment and upgrading, to maintain the desired EM and physical specification

over the equipment's lifecycle.

5. CONCLUSIONS

EMI-related aspects of functional safety cannot be verified solely by normal immunity tests. If it was possible to devise an immunity test plan that correctly addressed all of the issues – it would cost more, and take longer, than any organisation could afford.

Instead, methods similar to those already employed for other safety issues should be used – the application of well-proven and well-understood assessment and design techniques, backed up by tests that verify their suitability.

These good-EM-engineering-techniques should provide confidence that the equipment will function safely enough, over its lifecycle, considering its foreseeable exposure to electromagnetic, physical and climatic environments, reasonably foreseeable use/misuse and faults. Intentional EMI may also need to be taken into account.

This situation is similar to the one that faced safety-related software. As for EMC, it is totally impractical to prove that software is safe enough simply by testing it – it would cost more, and take longer, than any organisation could afford. So software experts have devised and validated appropriate design methods for achieving whatever safety integrity is required [8]. It is now time to do the same for EMC.

6. REFERENCES

[1] IEC 61508, *"Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems"*, (seven parts).

[2] Keith Armstrong, *"New Guidance on EMC-Related Functional Safety"*, 2001 IEEE EMC International Symposium, Montreal, Aug. 13-17 2001. Proceedings: ISBN 0-7803-6569-0/01, pp. 774-779.

[3] Keith Armstrong, *"New Guidance on EMC and Safety for Machinery"*, 2002 IEEE International EMC Symposium, Minneapolis, Aug. 19-23 2002. Proceedings: ISBN: 0-7803-7264-6, pp. 680-685.

[4] *"EMC for Functional Safety"*, IEE (London, UK) training course (first held February 10th 2004).

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

[6] IEC/TS 61000-1-2:2001, "*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."*

[7] Keith Armstrong, *"Review of Progress with EMC-Related Functional Safety"*, 2003 IEEE EMC Symposium, Boston, August 18-22 2003, Proceedings: ISBN 0-7803-7835-0, pp 454-460.

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

[9] Michel Mardiguian, *"Combined Effects of Several, Simultaneous, EMI Couplings"*, 2000 IEEE International Symposium on EMC, Washington D.C., August 21-25 2000, ISBN 0-7803-5680-2, pp. 181-184.

[10] Wendsche S. and Habiger E., *"Using reinforcement learning methods for effective EMC immunity testing of computerised equipment"*, Proc. Int. Symp. Electromagnetic Compatibility (ROMA'96), Rome, Italy, Sept 1996, pp.221-226

[11] Vick R. and Habiger E., *"The dependence of the immunity of digital equipment on the hardware and software structure"*, Proc. Int. Symp. Electromagnetic Compatibility, Beijing, China, May 1997, pp 383-386

[12] Jansson, L., and M. Bäckström, *"Directivity of Equipment and its Effect on Testing in Mode-Stirred and Anechoic Chamber"*, IEEE Int. Symposium on EMC, Seattle, WA, August 1999

[13] Freyer, G. J., *"Distribution of Responses for Limited Aspect Angle EME Tests of Equipment with Structured Directional Directivity"*, The 2003 Reverberation Chamber, Anechoic Chamber and OATS Users Meeting, Austin, TX, April 2003.

[14] Freyer, G.J., and Hatfield, M.O., *"An Introduction to Reverberation Chambers for Radiated Emission/Immunity Testing"*, ITEM 1998, The International Journal of EMC,1998.

[15] Freyer, G.J., *"Considerations for EMC Testing of Systems with Safety and/or Reliability Requirements"*, EMC Europe 2004, Eindhoven, The Netherlands, September 6-10 2004.

[16] ANSI/IEEE C62.41, *"Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits".*

[17] Simon J Brown and William A Radasky, *"Functional Safety and EMC"*, paper presented at the IEC Advisory Committee on Safety (ACOS) Workshop VII, Frankfurt am Main, Germany March 9/10 2004.

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

[19] W H Parker, W Tustin and T Masone, *"The Case for Combining EMC and Environmental Testing"*, ITEM 2002, pp 54-60.

[20] William A Radasky, *"An Update on Intentional Electromagnetic Interference (IEMI)"*, Interference Technology, Annual EMC Guide 2004, pp 217-220.

Many thanks to Simon Brown of the UK's Health and Safety Executive and to the many others who contributed to this paper.