(Title) Challenges in Testing

(Subtitle) Validation, Verification and Immunity Testing Techniques for EMC for Functional Safety

(Author) EurIng Keith Armstrong, Cherry Clough Consultants

Text as published in Conformity magazine, submitted September 2007

A system that could have an impact on functional safety, is 'safety-related,' or 'safety-critical' should maintain sufficiently low risks to users and third parties over its entire lifetime. It is usually required to be safe despite the occurrence of at least one fault, and also despite reasonably foreseeable misuse.

Complete safety systems can be single items of equipment, or at the other extreme they can be large networks comprising many items of equipment.

Where reasonably foreseeable EMI could affect the safety risks of such systems, they must maintain sufficient EM performance over their lifetimes.

This issue is usually called 'EMC for Functional Safety' – a very different discipline from compliance with EMC regulations, such as the European Union's EMC Directive. (See references [1-5] for additional information on this topic.)

The EM environment that such systems could experience over their lifetimes could be very different from that tested by standard 'EMC compliance' immunity tests. Nuclear electromagnetic pulse (NEMP or HEMP) or Intentional EMI (IEMI) can be of significant concern in some applications.

Physical and climatic environments, plus the wear and tear and misuse that systems can be subjected to over their lifetimes can cause circuit EM behavior to alter, and can degrade the performance of EM mitigation measures such as shielding, filtering, and transient suppression.

The EM performances measured by the normal 'EMC compliance' immunity tests are very poor indicators of real-life behavior, for reasons I've written about previously (see [6] and [7]). An EMC test plan that gave sufficient confidence for safety would be much too lengthy, and much too costly.

Just as for safety-related software (Part 3 of IEC 61805), appropriate EMC design techniques are required, based on qualitative and quantitative assessments of the reasonably foreseeable worst-case EM and physical environments over the lifetime of the system.

To achieve a suitable level of confidence in our equipment's EM performance within a reasonable cost and time budget, we need to employ appropriate EMC design methods as well as appropriate validation and verification methods (which include EMC testing).

IEC 61508 [8] is the basic IEC standard on Functional Safety, and applying it to safety systems tells us how to determine the safety integrity levels (SILs) we need for their safety functions, and then how we should design to achieve those SILs (e.g., how many redundant channels). But IEC 61508 does not tell us how to design or validate the EM performance.

IEC CD 61000-1-2 [11] is intended to become the International Electrotechnical Commission's basic standard on EMC for Functional Safety, to provide the 'pilot function' for all IEC standards on that topic. IEC CD 61000-1-2 can be read as the 'EMC Part' that is missing from IEC 61508, and includes validation and verification requirements, including testing.

Validation and Verification Techniques

A wide variety of validation and verification techniques can be used, including the following:

Demonstrations—Such as demonstrating that the functional safety requirements have been correctly implemented.

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

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

Reviews and Assessments—These ensure compliance with the objectives of each phase of the lifecycle. Usually performed by experts, on each phase of the lifecycle and the activities within them.

High SILs require greater confidence, and this can mean using third-party experts. A benefit of using reviewers from outside an organization is that it helps avoid the problems of 'institutional bias' or 'corporate blind spots.' Even where the reviewers are not as expert as the designers, their different perspectives will help detect problems.

Audits—These include checking that the correct specification, design, assembly, installation and verification processes have been followed.

Audits can be seen as a quality assurance activity and it helps if designers do not carry them out. Instead, people familiar with QA auditing, who are less likely to be distracted by design issues, should carry them out.

Non-standardized checks and tests–Because EMC testing has become standardised, many people tend to think of EMC testing only in terms of the standard test methods, such as MIL-STD-461, IEC 61000-4-x, etc. But there are very many non-standard EMC checks and tests that can (and often should) be done to improve confidence in safety integrity.

For example, a low-cost portable spectrum analyzer and close-field probe can be used to check the correct assembly of shielded enclosures, shielded connectors, and filters. This is a qualitative technique, rather than a quantitative one, but nevertheless can be very useful in improving confidence. It can also be usefully applied during the operational lifetime to check that shielding and

filtering performance is being maintained.

Similar close-field probing techniques can check purchased devices (e.g., integrated circuits) or equipment (e.g., power supplies, computers, etc.) to detect bad batches or errors in assembly, before they are incorporated into the safety system.

Many other EMC 'checking' methods can be designed and used to improve confidence without adding significant cost.

Individual and/or integrated hardware tests—Different parts of the safety system are assembled step-by-step, with checks and tests applied to ensure that they function correctly at each step.

Validated computer modeling—Computer-aided EMC design has made large strides in recent years, and is now routinely used in certain critical industries (for example, see [12]) to successfully reduce design and test timescales without sacrificing reliability. All computer modeling is based on simplifications, so it is important to validate any predictions by appropriate testing. But once the model is shown to replicate the test results with sufficient fidelity, it can be used to quickly simulate the results of numerous similar tests that would be too costly or time-consuming to perform in real-life.

Testing (e.g. factory acceptance test or on-site testing)—Most engineers automatically think of EMC testing as the only way to prove adequate EM performance. But as mentioned above, an EMC test plan that could – on its own – give sufficient confidence in EM performance for safety reasons, will always be much too lengthy and much too costly.

EM immunity testing is supplementary to the other validation and verification measures. Clause 9.1 of IEC CD 61000-1-2 says: "In most cases there will be no simple or practicable way to verify by means of testing that EM immunity is achieved." Despite this, appropriately-designed testing is a powerful validation/verification technique, and some suitable techniques are discussed below.

EM Immunity Test Methods

EM measures required for the achievement of adequate system safety should be evaluated using EM testing and highly-accelerated life testing (HALT), to demonstrate sufficient confidence that individual EM design aspects (e.g., circuit, shielding, filtering, surge transient or ESD suppression, etc.) will reliably achieve at least their minimum EM performance requirements over the anticipated lifetime of the final system.

Such tests should be carried out as early in a project as possible, to reduce technical risks and save time and cost. Some of them will not need to have a functioning unit available – for example the effectiveness of filters, and shielded enclosures, cables and connectors, can be tested in isolation.

It is also good practice to apply the immunity tests to the final safety system, after installation and commissioning. For smaller systems this may be possible in a test laboratory, but larger systems may need to be tested on site. On-site EMC test methods exist (such as those found in [13]), but some might prove too difficult, in which case they should be applied at the highest practica-

ble level of system integration. Care should be taken to apply them so that they realistically simulate the way in which EM phenomena will affect the whole system. For example, when testing systems that use redundant channels, all of the channels should be exposed to the EM environment simultaneously – testing one channel at a time proves nothing at all about the system's safety.

All immunity tests should be based upon accepted test methodologies, such as the IEC 61000-4-x series, or the test methods in MIL-STD-461, all of them modified as necessary to better simulate the real-life EM environment where the system is to be operated, and/or to improve confidence that the test results are meaningful for real-life safety.

For instance, the IEC's basic test method for radiated RF immunity, IEC 61000-4-3, is limited in terms of angle of incidence, frequency range, modulation type, modulation frequency, and numbers of simultaneous modulated frequencies, any or all of which could have a significant effect on the performance of electronic devices and software.

Real-life radiated RF environments are always more complex than those simulated by the unmodified IEC 61000-4-3 test method, and can cause very different and complex effects. Similar considerations apply to the other IEC 61000-4 series standards, and this problem is recognized in IEC CD 61000-1-2.

Equipment is especially susceptible at the operating frequencies of its internal hardware and software processes. But high-enough levels of interfering signals can overdrive devices, causing errors, malfunctions, maybe even damage, at any frequency.

A continuous RF test method currently used in some safety-critical industries uses unmodulated signals stepped in small increments over the range 0 to 30kHz, with a one-second pulse OFF then ON again at each step. Some test methods (e.g., IEC 61000-4-16) only test common-mode, whereas differential-mode tests may also be required to better simulate the effects of EM environment on the equipment.

Above 30kHz, the test signal at each frequency step has an unmodulated period, followed by 'chirp' modulation at least over the range of 'especially susceptible frequencies' below 30kHz, then is pulsed OFF for one second then back ON again using an unmodulated CW signal.

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 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, the testing time might be able to be reduced by modulating only at those frequencies, instead of a full chirp. Where exposure to pulsed sources is possible (e.g., radars, pulse weapons, etc.) their relevant frequency range should be covered using appropriate pulse modulation waveforms, especially any waveforms with a frequency content that includes any of the 'especially susceptible frequencies'. At each tested RF frequency, a CW test with a one-second pulse off and then on again is usually

required.

During immunity testing, all variations in functional performance should be recorded, and analyzed afterwards to see if they had any relevance for safety.

Physical Environment, Wear and Tear, HALT

The physical environment over the lifetime of the system can degrade its EM performance. Shock and vibration, bending forces, temperature extremes or cycling, wear and tear and many other lifetime mechanical, physical, climatic and biological influences can affect the radio-frequency (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.

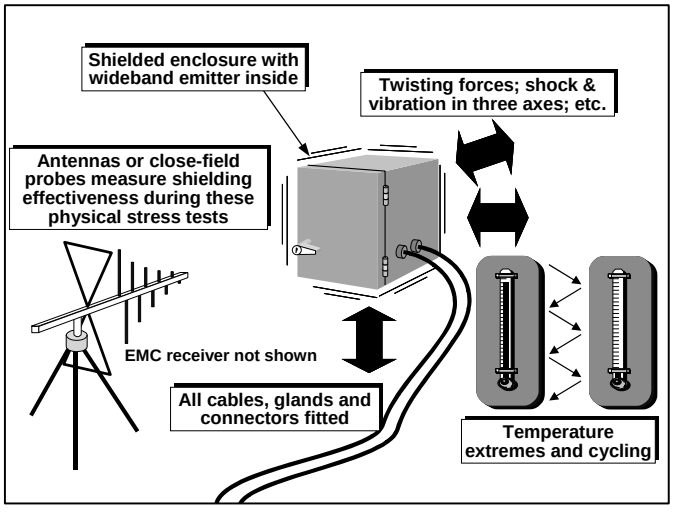
There are well-established test methods for most physical phenomena. HALT test experts combine physical test methods to quickly discover likely end-of-life characteristics.

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. It may be necessary to devise realistic tests for such physical lifetime stresses.

To verify that the EM design is adequate requires EM testing during the application of the physical stresses,such as mechanical forces, temperature extremes, etc. Appropriate close-field probing techniques can detect whether the EM performance of a shield or filter is significantly degraded by the physical stress. If degradation is to be permitted, more sophisticated quantitative measurements may be needed.

However, EM testing is only needed before and after HALT tests that simulate ageing and wear-and-tear.

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 itself, as shown in Figure 1, maybe using close-field probing of its seams, joints and other apertures, instead of the antenna shown.



(insert Figure 1 here)

Figure 1: EM testing during physical stress testing

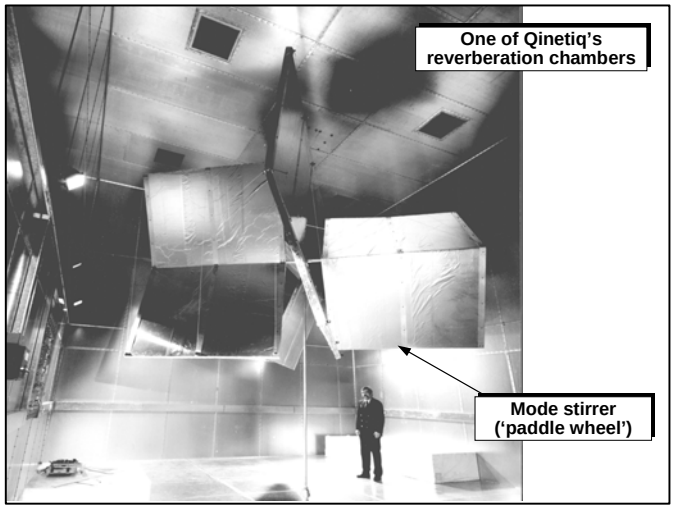
This has the advantage that the enclosure can be proved to be adequate as a parallel activity to the electronic and/or software design, helping to shorten timescales and reduce overall project costs.

HALT test plans should always be designed by HALT testing experts, based on the system's physical environment specification. Adding EM tests to these HALT tests need not add significantly to the overall time or costs, if they are designed appropriately.

Where suitable data exists or can be calculated for a particular EM design aspect, and when it is fully documented in the project's records, combined EM and physical testing may not be necessary. For example, tests such as those depicted by Figure 1 might not be needed where an enclosure manufacturer has already applied appropriate physical and HALT tests and measured their effect on EM performance (having first checked that the manufacturer's claims can be relied upon).

Reverberation Chamber Testing

Anechoic testing is unlike most real-life radiated EM environments, so reverberation chamber methods have been developed to give more confidence (see [14] [15] [16]). Unlike anechoic chambers, their results can be correlated mathematically with the reflectivity of the operational EM environment. Reverberation chambers and their RF power amplifiers cost a great deal less than anechoic chambers, and thorough testing can take less time than in anechoic chambers because there is no need to test with many angles, or with vertical and horizontal antenna polarizations.



(insert Figure 2 here)

Figure 2: Example of a reverberation chamber

A 'reverberation chamber' test method currently used for some safety-critical systems rotates the chamber's 'stirrer' or 'paddlewheel' over a full revolution using 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 'CW, chirp plus OFF/ON pulse', or other modulations, at a rate that is slow enough to be sure to detect any errors or malfunctions in the functions being monitored.

Where equipment is too large, or frequencies too low, or when testing on-site with no transmitting license, conducted coupling test techniques may be able to replace radiated methods. But conducted testing is not a true alternative to radiated testing, so it may be more realistic to use striplines, TEM cells, Helmholtz coils, or other test methods.

Test Levels and Uncertainty

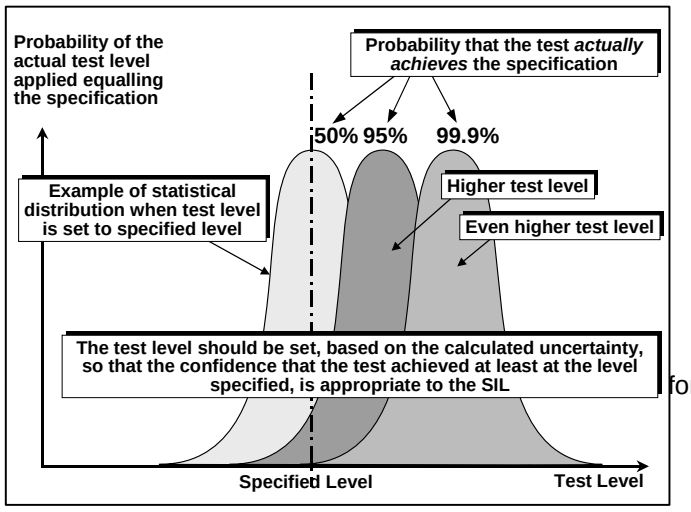
In the context of this article, SILs are measures of confidence that, when the EM or physical threats occur, they will not result in harm. So SILS are related to the design techniques used, and to the confidence achieved by the validation and verifications techniques employed.

To achieve a given level of confidence in EM and/or physical immunity testing, the EM and physical threat specifications will need to be higher than the environmental threats by a 'test margin' that takes care of the various uncertainties. There are uncertainties in the:

- Specifications of lifetime EM and physical threats;
- The stresses actually applied during immunity tests;
- Performance of individual units (e.g. due to component tolerances, variations in assembly and installation, etc.).

For example, MIL-STD-464 adds a 6dB test margin for safety-critical and mission-critical equipment, and a 16.5dB margin for ordnance.

Figure 3 shows that, when an immunity test is performed exactly at the specified threat level (for example, a test at 10V/m to simulate an RF field in the operational environment of up to 10V/m), there is only a 50% chance that the test was actually carried out at or above the desired level.



(insert Figure 3 here)
Figure 3: Uncertainty, statistics and test margins

There are standard methods for adding together various types of uncertainty, taking their type of statistical distribution into account (see, for example, [17]). Assuming a Normal (Gaussian) distribution (for example) in Figure 3, increasing the test level by one standard deviation improves the confidence that the test level reached/exceeded the specification to 68%, increasing by three standard deviations improves it to 99.7%, and four standard deviations achieves 99.99%.

The level of confidence achieved by the testing should generally be at least of the same order as the required SIL. For example, SIL 3 represents a probability of dangerous failure of a safety function 'on demand' or 'in a year' of between 0.01% and 0.1%, which is comparable with the 99.99% confidence given by testing with a level that is four standard deviations above the specified level.

To avoid testing at very high levels, with its attendant risks of over-design and unnecessarily high costs, it is important to use test methods and quality control that achieve low standard deviations.

Where the final safety system employs 'zones' protected by EM mitigation measures (e.g., filtering, shielding, transient suppression, etc.), some or all of the EMC tests applied to the equipment in the protected zones may not need to be as severe as the final safety system's overall EM specification.

For example, if the worst-case lifetime radiated RF threat, plus the test margin to achieve sufficient test confidence, required a test level of 1000V/m, employing an enclosure that can be relied upon to achieve at least 40dB attenuation (over the anticipated lifetime despite the worst-case physical environment) would require the equipment housed within it to be tested at only 10V/m.

The effectiveness of the mitigation measures also needs to be verified, but for techniques such as filtering or shielding over their linear regions there is usually no need to test at the worst-case levels plus the test margin. Their effectiveness in dB can be measured using low test levels.

Where appropriate data is provided with a purchased enclosure, it may not be necessary to test

the effectiveness of its EM mitigation at all. In such cases it is always necessary to ensure that the manufacturers' data can be relied upon.

Where it seems impossible to avoid RF testing at very high levels, reverberation chamber methods (such as those described in [18], or recommended for civil aircraft by [19]) can be much more cost-effective than 'traditional' anechoic chamber tests. Methods of using low-level RF tests to predict the outcomes of high-level tests, to avoid the cost of high-level tests, are being developed in IEC 61000-4-23 and by the military, and might be able to be used. Testing with high levels of surges and transients often requires finding or making suitable test equipment.

Because of the complexity and non-linearity of modern electronics, software and systems, passing an immunity test at the highest level does not always ensure that the test would be passed at a lower, more commonplace level. Confidence can be improved by repeating all types of immunity tests using a range of levels up to the highest.

Simultaneous Phenomena

Simultaneous phenomena are a feature of real-life EM environments (e.g., transmissions on multiple radio channels; continuous RF fields plus mains transients or ESD, etc.). They are also a feature of real physical environments (e.g., temperature plus vibration, temperature plus humidity, etc.). These issues should have been captured in the specification used to control the design and formulate the validation/verification plans.

Testing with multiple simultaneous RF threats is already used for testing military aircraft and digital TV receivers, and multiple-signal RF generators are commercially available. So testing using simulated real-life RF environments is an option that should be considered.

Testing that applies different types of phenomena simultaneously is not uncommon in physical/climatic testing, and is normal in HALT, but is (almost) unknown in EMC testing. Appropriate analysis techniques can generally be used to achieve sufficient confidence in safety performance despite simultaneous EM phenomena, without the need to test more than one phenomenon at a time.

However, it is possible to test with different types of EM phenomena at the same time, and some such tests might need to be employed in some cases, to improve confidence when higher SILs are required. Any such tests would need to be very carefully planned, to achieve the desired confidence without disproportionate increases in timescales and costs.

Emissions Testing

It is usually assumed that all that is needed for EMC for Functional Safety is to ensure that the final safety system is immune enough. But it is possible for the emissions caused by an item of equipment to exceed the levels and/or frequencies assumed when the intra-system effects were analyzed to help create the original EM specification.

So it is also important to employ validation and verification techniques like those discussed above, to ensure that the emissions from the parts of the overall safety system are within their design limits, after assembly, installation and commissioning. It is also important to have sufficient confidence (given the SIL required) that they will remain so over the system's anticipated

lifetime in its physical environment.

Testing for Faults and Misuse
The design of the system should have taken into account reasonably foreseeable faults, use and misuse, and the effects that these could have on EM performance and hence on the system's safety.

To achieve sufficient confidence in system safety, it may be necessary to devise verification methods to determine whether the design adequately deals with such events. For example, EM and/or physical checks and/or tests could be repeated whilst simulating the various faults, use or misuse.
Careful planning will be required to ensure that such tests add usefully to the confidence in the system's safety without disproportionate increases in timescales and costs.

Testing Safe Shutdowns, Alarms, and Similar
Safety engineers often seem not to care whether a system fails, as long as it remains safe enough. But in real life, a system that shuts down or alarms too frequently will cause annoyance and/or financial costs to its operators or owners, and is likely to be modified in an unapproved manner, for example by disabling the safety shut-down or alarm functions.

Such modifications by the user are a reasonably foreseeable outcome of unduly sensitive shut-down or alarm functions so, if an accident resulted, the system's manufacturer could possibly be found liable.

So where safety shut-down, alarm and similar protective functions are to be tested, they should be tested twice. One test is required to ensure that they do not operate when they should not; the second test is conducted with the safety faults simulated, to ensure that they will operate reliably enough when they should.

Verification After Installation
The design and validation/verification of the safety system are based on assessments of the worst-case EM and physical environments, which often include assumptions that should be verified after the system's installation. EM and physical mitigation measures can degrade over time, and certain assumptions will have been made in their design. EM and physical environments can also change unpredictably over the anticipated lifetime.

Safety is required over the whole lifetime of a system, so it can be necessary to verify the EM and physical environments, and/or performance of any mitigation measures, regularly throughout the life of the system. Automatic or manual methods may be used, taking appropriate actions to maintain the required safety levels when unanticipated events are detected.

Planning the Validation and Verification
In conclusion, it should be readily apparent that proving that a system's EM performance is adequate for lifetime safety requires a great deal more than simply asking a test laboratory to perform some standard EM tests on shiny new equipment.

The planning of the validation and verification techniques needs to be performed by competent

and knowledgeable personnel, in parallel with the design phase. It can be possible to avoid lengthy test sequences by doing the design in a different way. Since no organization can afford the time and cost of an EM test plan that, on its own, gives sufficient confidence for the SIL required, it is necessary to use a wide range of design, validation and verification techniques to reduce the amount of standardised EM testing whilst achieving the required level of confidence in functional safety performance over the anticipated lifetime.

Keith Armstrong *is the principal of Cherry Clough Consultants, and can be reached at keith.armstrong@cherryclough.com.*

References

[1] The IET, “Guidance on EMC and Functional Safety”, 2000, http://www.theiet.org/publicaffairs/electro/index.cfm.

[2] Keith Armstrong, “New Guidance on EMC-Related Functional Safety”, 2001 IEEE International Symposium on EMC, Montreal, August 13-17, ISBN 0-7803-6569-0, pp. 774-779.

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

[4] Keith Armstrong, “Review of Progress with EMC-Related Functional Safety”, 2003 IEEE International Symposium on EMC, Boston, August 18-22, ISBN 0-7803-7835-0, pp. 454-459.

[5] Keith Armstrong, “EMC for Functional Safety”, (half-day paper), 2004 IEEE International Symposium on Product Safety Engineering, Santa Clara, August 13-15.

[6] Keith Armstrong, “Why EMC Immunity Testing is Inadequate for Functional Safety”, 2004 IEEE International Symposium on EMC, Santa Clara, August 9-13 2004, ISBN 0-7803-8443-1, pp. 145-149. Also: Conformity, March 2005, pp 15-23, http://www.conformity.com.

[7] Keith Armstrong, “Functional safety requires much more than EMC testing”, EMC-Europe 2004, Eindhoven, September 6-10 2004, ISBN: 90-6144-990-1, pp. 348-353.

[8] IEC 61805 (7 parts) “Functional safety of electrical, electronic and programmable electronic safety-related systems”.

[9] Keith Armstrong, “Design and Mitigation Techniques for EMC for Functional Safety”, 2006 IEEE International Symposium on EMC, 14-18 August 2006, Portland Oregon, ISBN: 1-4244-0294-8.

[10] Keith Armstrong, “Specifying Lifetime Electromagnetic and Physical Environments – to Help Design and Test for EMC for Functional Safety”, 2005 IEEE International Symposium on EMC, Chicago, Aug 8-12, ISBN: 0-7803-9380-5, pp. 495-499.

[11] IEC CD 61000-1-2 December 2006, “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”.

[12] Ian MacDiarmid of BAE Systems, EMCIA presentation, 14 December 2006, http://www.emcia.org.

[13] EMC Test Labs Association, TGN 49, Technical Guidance Note on On-site EMC Testing, http://www.emctla.co.uk.

[14] L Jansson, and M Bäckström, “Directivity of Equipment and its Effect on Testing in Mode-Stirred and Anechoic Chamber”, IEEE International Symposium on EMC, Seattle, August 99.

[15] G J Freyer, and M O Hatfield, “An Introduction to Reverberation Chambers for Radiated Emis-

sion/Immunity Testing", ITEM 1998, http://www.rbitem.com.

[16] John Ladbury, "Coupling to Devices in Electrically Large Cavities, or Why Classical EMC Evaluation Techniques are Becoming Obsolete", IEEE International Symposium on EMC, Minneapolis, Aug 02, ISBN: 0-7803-7264-6.

[17] CISPR 16-4, "Specification for radio disturbance and immunity measuring apparatus and methods. Uncertainty in EMC measurements".

[18] IEC 61000-4-21, Electromagnetic compatibility (EMC). Testing and measurement techniques. Reverberation chamber test methods.

[19] RTCA/DO-160, Civil aerospace EMC standards, http://www.rtca.org.

[20] IEC 62002:2006, "Mobile and portable DVB-T/H radio access. Interface conformance testing".