Another EMC resource
from EMC Standards

Opportunities in the Risk Management of EMC

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

Opportunities in the Risk Management of EMC

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

***Abstract* – It is not an exaggeration to say that we are witnessing the birth of a brand new industry – Risk Management of electromagnetic compatibility (EMC) – which will be needed in most safety-related and high-reliability applications/industries.**

But at the moment there are (effectively) no resources available that can satisfy its requirements, either from EMC test laboratories or functional safety assessors.

A great deal of work needs to be done to prepare manufacturing industry, test laboratories and safety assessors for these requirements, for which a large demand will build up by 2021.

The new opportunities now available include:

- **Academic teaching at all levels**
- **Academic research**
- **Vocational training courses**
- **Computer-aided simulation**
- **Test methods and specialized test equipment**
- **Verification/validation techniques other than testing**
- **Development of policies and procedures**
- **Safety Assessor services**
- **Accreditation services**

This paper briefly introduces the rapidly growing need for the above, and discusses each of these opportunities in turn.

***Keywords* – EMC, EMI, functional safety, high-reliability, mission-critical, reliability, risk analysis, safety-related, safety-critical, security, safety risks, SmartGrid, automobiles, medical devices, service robots.**

I. Introduction

It has now been firmly established that no practicable amount of EMC immunity testing, at any increased test level, is sufficient on its own to provide the levels of confidence required where an error or malfunction in electronics can result in unacceptable levels of safety risk [1] - [12].

Similar arguments apply to mission-critical systems, legal metrology, and national defense and security, some of which may require levels of reliability that exceed those of most safety requirements.

Electronics – and the software and firmware that runs on them – have been a concern for functional safety risks since they started to be used in industrial automation, drive-by-wire and fly-by-wire applications, amongst others, in the 1990s.

At the time of writing, electronic technologies (and software and firmware) are poised to take huge steps in the next decade, exposing the developed world to historically unprecedented safety risks, these include:

- Continuing automation of automobiles and trucks, leading to totally automated vehicles and highways.
- SmartGrid, which will place many domestic (household) appliances under remote control.
- Many infirm and elderly people "cared for" directly by "Service Robots". There could be many millions of them in use by 2020, initially in Japan [13].
- New nuclear. Existing nuclear plant rely mostly on analogue and relay technologies, but new plant will use computer technology for control and safety.

These are not "pie in the sky" applications – they are very real, with standards and products being developed now in the USA, Japan and Europe. By 2021 they will almost certainly be an everyday reality for most of us in the developed world.

In the 1990s a very great deal of work in academia and industry resulted in the development of IEC 61508:2000 [14] (since superseded by its Edition 2:2010) to control such risks.

However, [14] did not specify how to correctly deal with EMC, which was left to the team who created IEC TS 61000-1-2:2000 [15] (since superseded by Ed2:2008). Complying with Ed.2 of [14] requires compliance with Ed.2 of [15]

At the time of writing, the following standards and standardization projects require EMC Risk Management:

- IEC CD 60601-1-2 Draft Ed.4:2010 [16] EMC for Medical Equipment and Systems. Since IEC 60601-1 Ed3 all related standards have to embody Risk Management in controlling safety risks.
- IEC TS 61000-1-2 [15]. This is progressing towards full standard status as the IEC's Basic Standard on EMC for Functional Safety.
- IEC CD 61000-6-7, Draft Ed.1 [17] 2010 The "Generic Standard" on EMC testing for Functional Safety. A number of new product standards on EMC for Functional Safety are awaiting its publication.
- DEF STAN 59-411, the UK defense industry's EMC standard.
- ISO 26262 (draft) [18]. This is being developed from IEC 61508 as the automotive industry's functional safety product standard. At the moment it hardly mentions EMC, and even then simply assumes that immunity testing is sufficient – which of course it is not, at any test level [10]. This will have to be modified to require compliance with [15] too, if it is to achieve recognition as a product standard

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

developed from IEC 61508.

- IEC 61326-3-1/2, EMC for functional safety for electrical equipment for measurement, control and laboratory use. Although these two standards only describe immunity test requirements, they should be used within a risk management framework governed by IEC 61508 and IEC 61000-1-2.

Many safety-related industries already require equipment and systems to comply either with [14] or with product standards developed from it. Complying with its 2nd Edition requires compliance with Ed2 of [15] – so there is an existing need for verification, validation, and assessment services to the requirements of [15] that will grow with time as product standards are updated to bring them into line with Ed.2 of [14].

[8] is a practical guide to compliance with [15] and has been very heavily downloaded worldwide, encouraging the application of [15].

The new opportunities now available include the development and provision of:

- Academic teaching at all levels
- Academic research
- Vocational training courses
- Management policies and procedures
- Computer-aided simulation
- Test methods
- Test equipment
- Verification/validation techniques other than testing
- Laboratory accreditation
- Safety Assessor services

Many safety experts are still uncomfortable with functional safety issues, and most safety test lab managers know very little about them, because they employ statistical methods, rather than simply (for example) measuring creepages and clearances or testing voltage withstand. In general, it is found that most functional safety and "ordinary safety" practitioners and their managers know little about real-life electromagnetic interference (EMI), even when they manage both the EMC and safety test labs in their organization, and even less about how to combine statistical risk management with EMC.

Also, most EMC experts, test lab managers and design consultants know very little indeed how to risk-manage EMC for compliance to Functional Safety standards such as [14].

Many of them still believe that all one has to do for whatever level of safety is simply apply the normal EMC tests at higher levels, to a few brand-new fault-free examples of equipment in a benign physical and climatic environment, as the auto industry does.

And no independent Safety Assessment Body or Independent Safety Assessor (ISA) yet has the skills to deal with the risk management of EMC. The author knows this for a fact because he has spoken on this topic at meetings and conferences held by Independent Safety Assessors, for example [19].

There will be a huge demand for skills and services in this new industry of risk-managing EMC, but at the time of writing there are only a very few individuals worldwide who could provide them.

The following Parts of this paper deal with each of the opportunities listed above, in turn.

II. Academic Teaching

Academic courses on risk management of EMC will be required at undergraduate and postgraduate levels, and will in turn require appropriate text books.

Courses will be required at all levels, from merely raising the awareness of the issues, to providing detailed and comprehensive skills for those who will be involved with safety-related systems as designers, managers and assessors.

First Degree and Master's levels will be suitable for most designers and managers – but where very high value, very high risk projects such as high-speed rail networks, nuclear plant, space vehicles, national security, automated highways, Smartgrid, service robots, etc., are concerned – manufacturers, owners and government agencies will prefer people with Doctorates in the required areas.

III. Academic Research

There are many areas in which research will be required, to support the demand for new understanding and techniques in design analysis and simulation – for equipment and systems of any scale, plus new tools for design verification.

These new techniques and tools will mostly be software based, but – as later Parts show – there will also be some research needed on new test methods and test equipment.

IV. Vocational Training Courses

Courses will be required in two main areas:

i) Educating designers in good EMC and safety design techniques, and their managers in how to manage them effectively

ii) Educating testers and Safety Assessors in appropriate verification and validation techniques

These will generally be provided by organizations that are outside the academic world, for the upskilling and continuing-professional-development (CPD) of every sort of designer, manager and safety assessor.

There are many tens – if not hundreds – of thousands of people worldwide already active in safety-related applications of electronics (and software), who will need these courses.

V. Management Policies and Procedures

The cost-effective application of risk management to EMC will require appropriate management policies and procedures.

These policies and procedures will also be required to defend against product liability claims based on EMI causing unacceptable safety risks.

Volume manufacturers will generally require a single policy and procedure that covers their complete operations, whereas custom engineers and system integrators may have a single

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

policy but may need to employ different procedures for different projects.

Owners of safety-related systems will need management policies and procedures on the risk management of EMC, to assist the tendering process, validate what is supplied, and maintain the safety of their systems over their lifecycles.

Safety assessors will need policies and procedures to cost-effectively control their services in the risk management of EMC, and to gain accreditation for those services.

Government safety agencies will also require appropriate policies and procedures to enable them to protect the public from manufacturers who do not understand that EMC immunity testing is insufficient for controlling safety risks [1] –[11].

VI. COMPUTER-AIDED SIMULATION

Here are some examples of what is needed to support this new industry, for equipment and systems where the safety risks rely upon correct operation of hardware or software (i.e. where low-technology "fail-safes" or "backup systems" are not used, or would cause too much downtime):

a) Identifying systematic noise "spikes"

Combining software simulators with field solvers would make it possible to design software compilers, integrated circuits, printed circuit boards (PCBs), equipment and systems of any size that will minimize their systematic (intrasystem) noise and thereby maximize their noise margins.

Such simulators would be very useful for improving the cost-effectiveness of "regular" EMC design anyway, but the particular focus of this new industry will require the control of transient EMI that would not be detected by practicable and affordable EMC testing.

The problem here is that a short "spike" in systematic noise – often caused by several output transistors switching simultaneously, can cause a transient degradation in the digital noise margin causing one or more bit errors.

Such spikes might only occur very infrequently, and – if they cannot be predicted – massively-extended immunity test times would be required where testing was used as the method of demonstrating the required confidence in complying with the target risk level.

Increasing continuous immunity test times by 10 or more, to cover all possible modes of software execution, would not be an unreasonable expectation for a typical product, but some systems (e.g. road vehicles) are so complex that much longer test times would be required.

And when we consider that transient noises (e.g. fast transient bursts, surges, ESD, etc.) might occur at the same time as the spike in the systematic noise, then transient testing times may need to be increased by much more than 10 times even for simple products.

Whilst the number of transients currently applied during testing are evidently sufficient to provide manufacturers with products that are reliable enough as regards warranty costs, downtime and customer satisfaction, it can easily be shown that the testing time would need to be increased by a factor of 100 or more to begin to even approach the confidence factors considered usual for controlling safety risks.

IEC 61508 calls these confidence factors "SILs" (for safety integrity levels) and the SIL appropriate for the safety systems for a nuclear power plant (SIL4) corresponds to a confidence level of between 99.99% and 99.999% [12]. Compare this with the approximately 80% confidence assumed to be achieved by correctly applying the regular EMC immunity test, for example, provide a presumption of conformity are required with the non-safety-related European Union EMC Directive, 2004/108/EC.

Clearly, such increases in testing time would not be practicable, and the "brute-force mitigation" alternative of applying very high-specification shielding and filtering is not always practicable or cost-effective – hence the need for a simulator that can identify the systematic noise caused by a given software operating on a given hardware platform.

Simulators that identified spikes in systematic noise would allow software and hardware to be modified to reduce their degradation in noise margins. Showing that a design's systematic noise margin did not suffer from untoward levels of spikes would make it possible to use affordable EMC test plans when verifying and validating safety-related designs.

By identifying the software events that caused systematic noise spikes, simulators would also make it possible to ensure that those software events were exercised during immunity testing, and/or make it possible to design EMC test instruments that triggered off those software events, again making it possible to use affordable EMC test plans when verifying and validating safety-related designs.

b) Identifying susceptibilities

Systematic noise spikes are only one of the ways in which electromagnetic (EM) disturbances external to a device, product, equipment or system can cause interference.

Combining software simulators with field solvers would also make it possible to discover how wanted signals could be corrupted by the noises created by EM disturbances.

This is similar to a) above, but in this case it is the time/phase relationships between the interfering noises and the wanted signals that are analyzed.

Certain noises, if they occur in a particular time or phase relationship with a digital or an analogue signal, can cause incorrect data. For example, noise that occurs at frequencies:

- very close to clock frequencies or their harmonics
- within the range of analogue amplifiers (considering both their linear and non-linear modes of operation)
- very close to analog-to-digital sampling frequencies, or their harmonics
- close to the electrical resonances that occur in conductive structures, including structural metalwork, conductors, PCB traces, and circuits that employ reactive components
- close to the mechanical, hydraulic or pneumatic resonances of sensors or transducers (e.g. mechanical

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

resonance of a spring-damper-wheel system; hydraulic "hammer", etc.).

The last point in the above list would require a "multi-physics" simulator.

Testing all possibilities would clearly take much too long, and (as before) "brute-force mitigation" may not be practicable or cost-effective.

Also as before, identifying problems allows modification of software and hardware to reduce EMI possibilities, and allows test instruments to be triggered by sensitive signal states to ensure that immunity tests are applied to the worst-cases for susceptibility, without having to increase testing times.

Once again, the aim is to significantly increase confidence in the correct and reliable operation of the software, for example by 10 or more times, but without significantly increasing immunity testing times beyond what is typically done at the moment.

c) Simulating the "emergent properties" caused by system integration

The purpose of this new type of EMC simulator is to increase the confidence that equipment and/or subsystems can be integrated into large systems without compromising the risks.

It is commonplace to construct large systems and installations from smaller items, but the problem of "emergence" means that they do not always behave as one would expect.

The smaller items will probably have passed EMC tests, and the common assumption is that the finished system would therefore also meet similar EMC requirements – if it were possible to test it. This is, of course, little more than wishful thinking, due to interactions between system components that were not assessed during their individual EMC tests.

At the moment the only alternative is to do costly on-site or whole-vehicle EMC testing, which is necessarily limited due to time and cost and cannot (on its own) reach the kind of confidence necessary for validation of safety-related systems (or other systems with tough reliability criteria) as shown by [1] – [11].

Simulation tools that helped improve confidence in the reliability of integrated systems will help save considerable time and cost in system design, verification and validation.

VII. TEST METHODS

Although EM immunity testing can never be sufficient for demonstrating the high reliability required for safety-related systems and many other types or equipment or system, it is still a powerful and important verification/validation method.

To achieve confidence for reliability issues that cannot be adequately addressed by other methods, we need to develop immunity test methods to improve "test coverage".

An improvement in test coverage can be achieved by using the "normal" test methods, but modifying them a little, for example by applying the normal continuous RF conducted and radiated immunity tests with a variety of different modulation frequencies or types likely to hit the most susceptible frequencies (where we know what they are) as recommended in clause A.5.20 of MIL STD 461F [20], and on pages 20-11 and 20-13 of RTCA DO160F Section 20 [21].

Another easy technique is to increase the time taken by continuous or transient tests, for example by testing more modes of operation, so that they are more likely to "hit" one of the especially susceptible software events.

However, such methods can easily quadruple the costs of testing, and if they increase the confidence that reasonably foreseeable EM disturbances will not cause safety hazards by a factor of four, it still leaves most types of EMC test at least one order of magnitude short of proving that a design will be safe or reliable enough in real-life, over its operational life-cycle.

It is worth noting that the recent IEC work on high-power EM disturbances (HPEM) and their mitigation, especially as regards systems and national infrastructures, which has resulted in many new IEC standards in recent years, is also an EMC risk management issue. Although it is not generally presented as being associated with the control of safety risks, this work is relevant for this new industry.

Existing single-frequency continuous RF tests are incapable of testing intermodulation effects, yet in real life equipment is often exposed to two or more RF signals at significant levels, causing intermodulation.

The design of shielding, filtering, and software to pass the usual immunity tests therefore does not ensure adequate control of EMI caused by intermodulation. Even if this is considered to have proven acceptable, so far, for reducing warranty costs and downtime to commercially-acceptable levels, [12] shows that it does not even come within at least one order of magnitude of providing sufficient design confidence for any safety-related system (as defined by [14]).

Alistair Duffy and Antonio Orlandi have demonstrated a reverberation chamber test method that shows promise for testing radiated field immunity with more than one simultaneous RF frequency to test intermodulation effects [22] [23].

The author has recently started collaborating on a "twin-tone" RF immunity test method for just this reason, for conducted and radiated tests. This new method promises to dramatically increase test coverage with very little extra cost in test equipment and no increase in testing time.

Others have also begun to think about other test methods to increase confidence in real-life exposure to EM disturbances, without adding significantly to test times and costs.

It would be wonderful if a new test method significantly increased the confidence in a design's levels of safety risks while also being able to be used for "regular" compliance testing.

Some of these new test methods might have to be listed by IEC or ISO as being suitable for safety risk control purposes only. But even if they are not listed by these standards organizations at all – this will not matter if a safety system designer or assessor considers them to be a valid way to increase the confidence in a design.

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

VIII. TEST EQUIPMENT

The above discussions on new computer-aided simulators and test methods have mentioned some possibilities for new test equipment.

When the test equipment manufacturing community start to take notice of this new requirement for risk-managing EMC, and understand how very little design confidence is achieved by the regular EMC test methods, the author expects them to develop many new and useful types of test and test methods very quickly.

In addition, some projects will require special test equipment to verify and validate specific issues that cannot be dealt with by other techniques, usually because the technologies concerned are too new for there to be any consensus on what constitutes good design practice.

At the moment, such test equipment is mostly constructed ad-hoc by test laboratories or EMC consultants, but there will be opportunities for test equipment manufacturers to offer customized versions of their own products and/or "one offs", for specific customers' needs.

Note that most EMC test equipment is designed to comply with certain CISPR, IEC or ISO test standards. Where increasing the confidence in a design's levels of safety risks uses customized or one-off test equipment, compliance with these EMC test standards will often not be necessary – and might not even be possible – but this should not matter as long as good, repeatable EMC testing practices are followed.

IX. VERIFICATION/VALIDATION TECHNIQUES

Because no one verification method (e.g. immunity testing) can provide sufficient confidence in the levels of safety risk for safety-related systems that rely upon complex electronics (and their software or firmware), it is necessary to use a number of different techniques.

It is as if each technique was a spotlight that illuminated certain aspects of a design very well indeed, but left much of the design in shadow. By shining a number of spotlights from many different angles, we highlight many more design aspects, increasing our confidence that we know as much as we need to for ensuring safety risks are as low as required.

[15] requires the use of proven design techniques for EMC hardening and error detection or correction, plus a range of verification and validation techniques, including (but not limited to) the following:

i) Demonstrations

Showing others that the reliability requirements have been correctly implemented in the design, using any available methods.

ii) Checklists

Checklists capture an organization's unique expertise, developed by many people over many years on their products and application areas. Ensuring that none of these hard-earned lessons are overlooked, or implemented incorrectly on new products, helps increase confidence in their reliability and safety.

iii) Design Reviews and Assessments

Staged activities usually associated with "signing off" a project phase. They aim to ensure that EMC and safety design measures have been observed, applied and implemented correctly, and are usually performed by experts in the necessary disciplines.

iv) Audits

Including checking that correct specification, design, assembly, installation, verification and validation processes have been followed. A QA activity.

v) Inspections

For example, checking that assembly and installation have followed the EMC requirements correctly. Another QA activity.

vi) Non-standardized checks

Many non-standard EMC tests ("checks") can (and often should) be used or developed to improve confidence in lifecycle reliability, often without adding significant delays or costs.

vii) Individual and/or integrated hardware tests

Different parts of the equipment or system are assembled step-by-step, with appropriate checks and tests applied at each step. Most appropriate for large systems or installations.

viii) Validated computer modeling

Computer-aided EMC design is now routinely used in some critical applications 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.

ix) Testing (e.g. factory acceptance or on-site testing)

The final product or system is tested for immunity at the highest practicable level of assembly, either in its manufacturer's factory, or *in-situ*.

The software industry went through exactly the same exercise in the 1990s, when they realized that it was impossible to do enough testing for safety-related systems.

They ended up with requirements for using proven good design techniques, plus a number of additional verification and validation techniques similar to the above list, now embodied in [14] (actually, in its Part 3).

Now it's the turn of the EMC industry to embrace this approach.

X. SAFETY ASSESSOR SERVICES

When IEC 61508 was first published in 2000, there were no organizations capable of assessing hardware or software for functional safety, but by 2005 such services were available

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

world-wide from organizations accredited for just that purpose, and various industry-self-regulation associations had been created (e.g. “The 61508 Association”).

No doubt some EMC test labs will branch out into design assessment and associated risk management compliance services, and no doubt some functional safety assessment companies will develop EMC Risk Management skills.

And no doubt some safety assessors will learn to use EMC immunity testing for issues that are insufficiently covered by other verification and validation methods. This will make the life of the EMC test lab manager more interesting, and possibly increase lab income too, as EMC labs get more involved in designing customized test plans, customized tests themselves, and carrying them out.

There will also be a corresponding increased need for specialized/customized EMC test equipment.

XI. Accreditation Services

Organizations that provide verification and validation services in the risk management of EMC will want to be able to show they are “approved” by Safety Accreditation Bodies, which in some countries are aspects of government.

Of course, accreditation bodies charge for their services, and this new industry opens up more opportunities for them.

XII. Conclusion

A great many opportunities, for everyone from academic institutions to test equipment manufacturers; result from the upcoming new industry in risk managing EMC.

References

[1] Keith Armstrong, “New Guidance on EMC-Related Functional Safety”,2001 IEEE International EMC Symposium, Montreal, Aug. 13-17, ISBN 0-7803-6569-0/01, pp. 774-779.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] Keith 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.

[7] Keith Armstrong: “EMC in Safety Cases – Why EMC Testing is Never Enough”, Defence & Avionics session, EMC-UK 2007 Conference, Newbury, UK, 17 Oct. 2007

[8] “EMC for Functional Safety”, Edition 1, August 2008, The Institution of Engineering and Technology (IET, formerly the Institution of Electrical Engineering, IEE; London, UK) available: www.theiet.org/factfiles/emc/emc-factfile.cfm and www.emcacademy.org/books.asp.

[9] 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.

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

[11] W. Radasky, J. Delaballe, K. Armstrong, “Workshop on Achieving EMC to Help Control Functional Safety Risks”, Asia-Pacific EMC 2010, Beijing, April 12-15, 2010

[12] Keith Armstrong, “Including EMI in Risk Assessments”, 2010 IEEE International EMC Symposium, Fort Lauderdale, FL, July 25-30, 2010, ISBN: 978-1-4244-6307-7

[13] Private correspondence, National Institute of Occupational Safety and Health, JAPAN, July 2010

[14] IEC 61508 Ed.1, 2000, basic safety publication, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems”, (seven parts), http://webstore.iec.ch.

[15] IEC TS 61000-1-2, Ed.1, 200, 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.

[16] IEC CD 60601-1-2 draft Ed. 4.0, 2010, “Medical Electrical Equipment – Part 1-2: General requirements for basic safety and essential performance – Collateral standard: Electromagnetic compatibility – Requirements and tests”.

[17] Draft IEC 61000-6-7, “Generic Standards – Immunity Requirements for Safety-Related Systems and Equipment Intended to Perform Functions in a Safety-Related System (Functional Safety) in Industrial Environments”, IEC TC 77/389/CD, November 19, 2010.

[18] ISO/DIS 26262, “Road vehicles - Functional safety”

[19] Keith Armstrong, “The New IET Guide – How to do EMC to Help Achieve Functional Safety”, in “Making Systems Safer”, C. Dale and T. Anderson (eds), Proceedings of the Eighteenth Safety-Critical Systems Symposium, Bristol, UK, 9-11 February 2010, DOI 10.1007/978-1-84996-086-1_12, Springer-Verlag London Ltd 2010

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

[21] 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.

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

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

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