Why EMC Immunity Testing Is Inadequate For Functional Safety

by Keith Armstrong

(as printed in Conformity magazine, March 2005, a reprint of "Why EMC Immunity Testing is Inadequate for Functional Safety", 2004 IEEE Int'l EMC Symposium, Santa Clara, Aug. 9-13 2004, ISBN 0-7803-8443-1, pp 145-149, with the IEEE's kind permission)

Safety-implicated, safety-related, and safety-critical systems are increasingly using electrical, electronic and programmable electronic devices. All such devices can suffer malfunctions or damage due to electromagnetic interference.

Safety systems have safety integrity requirements (defined by IEC 61508 [1]), but their EMC aspects are not adequately controlled by either safety or EMC standards.

We discuss the shortcomings in the way that the EMC immunity of such equipment is dealt with, and shows that the normal immunity testing approach is inadequate, on its own, as a means of verifying this aspect of safety integrity.

Introduction

The cost of digital processing power, and the cost of solid-state power conversion, is continually decreasing. Consequently, electronic devices are increasingly used in safety-implicated, safety-related and safety-critical applications, especially in industrial, commercial, medical and transportation control and automation applications. The accuracy and reliability of these electronic devices is a concern for functional safety.

All electronic technologies are inherently prone to suffering from inaccuracy, malfunction, or even permanent damage when interfered with by electromagnetic (EM) disturbances in their operating environments. The continued shrinking of the silicon features in modern electronic devices makes them more powerful and less costly – but this shrinkage and its associated lower operating voltages makes the devices more susceptible to EM interference (EMI).

The intensity and frequency range of EM disturbances in the environment are getting worse all the time, due to the increasing use of digital, switch-mode, and wireless technologies. Combined with the increasing susceptibility of electronic devices to EMI, the reliability of electronic devices is inherently decreasing and this has important consequences for functional safety.

EMC standards and regulations have grown up around issues of spectrum control, and do not (in general) try to address safety issues. Safety standards and regulations generally have very poor coverage of EMI related issues. Manufacturers employing electronic devices in safety-implicated/ related/critical systems have therefore had little in the way of standards and regulations to guide them, and since many of them aim for the lowest possible cost and compliance with the minimum regulatory requirements it appears that functional safety problems are becoming increasingly likely, as shown by Figure 1.

Noticing the lack of standardization on "Electromagnetic Compatibility (EMC) for Functional Safety", the IEE (London, UK) set up a Working Group that produced a "professional guide" on this topic in 2000 [2]. This guide adopts a hazards and risk assessment based approach to the issue, and has since been utilized by at least one other professional body [3] in formulating its own guidance on this issue. In 2004 the IEE began to run a series of training courses on "EMC for Functional Safety" [4].

In the European Union (EU) the safety directives that require CE marking are "total safety" directives and so cover any/all functional safety problems caused by EMI – but neither they nor their listed harmonized standards say how this should be accomplished. Since the Electromagnetic Compatibility

Directive (EMCD) and its standards do not cover safety issues [1], this all leaves a great big gap in the control of an increasingly important safety issue.

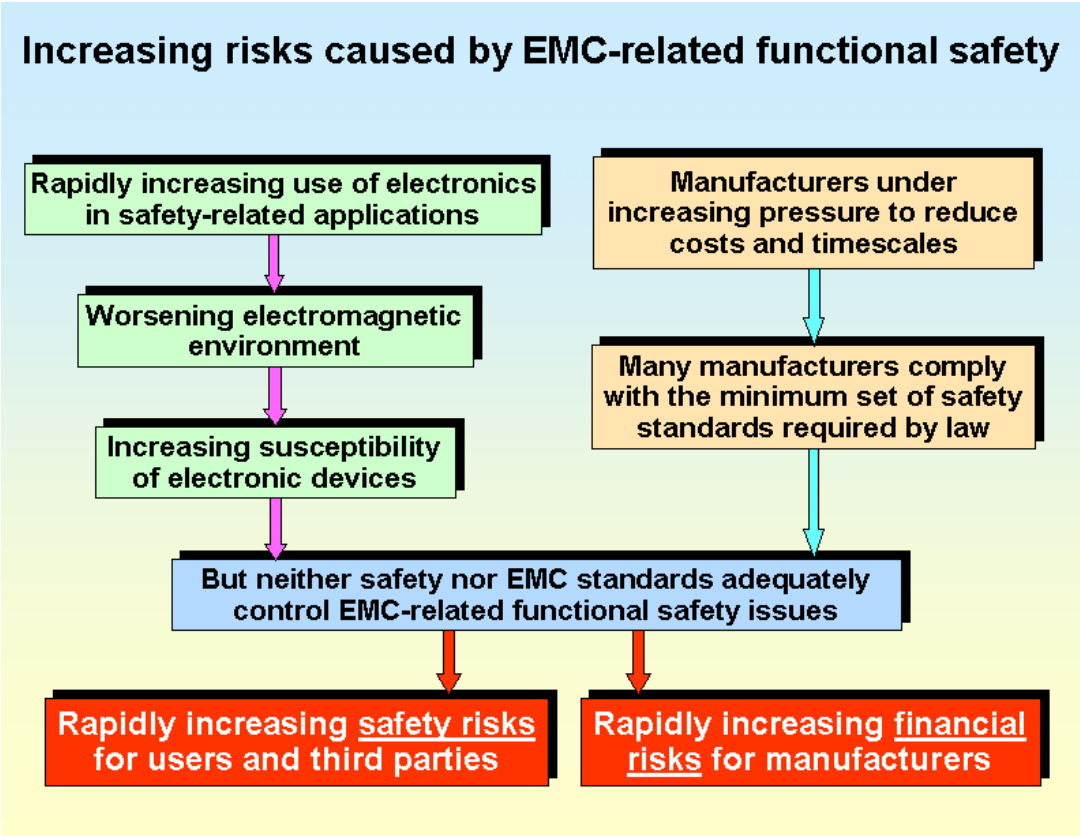

Figure 1

IEC 61508 [1] is the recent "basic IEC standard" that covers the functional safety of electronic and programmable equipment, but although it requires EMC to be taken into account it does not say how this should be done. However, since IEC 61508 employs a hazards and risk assessment based approach and an emphasis on safety by design rather than testing, for software as well as for hardware, it seems safe to assume that it would expect 'EMC for functional safety' to be treated in a similar manner.

IEC/TS 61000-1-2:2001 [5] is a recent IEC Technical Specification that covers EMC for Functional Safety, and is intended to become the basic IEC standard on this topic, possibly providing the EMC requirements that are lacking in IEC 61508. This IEC/TS employs a hazards and risk assessment based approach, similar to the IEE's 2000 guide.

Some IEC product safety committees have recently begun to add EMI-related functional safety requirements to their standards. But instead of following the hazards and risk assessment based approach employed by the IEE's guide, IEC/TS 61000-1-2:2001, and IEC 61508 they are all simply adding EMC immunity tests similar to those used for compliance with the EMCD [6].

This is unfortunate because, as the rest of this paper will show, EMI/EMC testing is inadequate when used as the sole means of achieving (or demonstrating) that an acceptable level of EMC-related functional safety performance has been achieved.

The EMC performance of equipment has traditionally been verified by testing one sample (or a few samples) of a new product or equipment in an EMC test laboratory. The test standards employed do not define any aspects of design or construction, and as a result this type of testing is sometimes called "black box testing".

However, the safety performance of equipment is traditionally verified by quite different means:

- The design is inspected against a number of safety design criteria, well-proven to provide a sufficient level of protection over the anticipated lifecycle, taking into account the range of the physical environment (e.g. temperature, vibration, pollution) and reasonably foreseeable use;
- Samples are tested to see if any foreseeable single fault could result in a dangerous condition ("single-fault safety");
- Every item of equipment that is manufactured is put through basic tests that check whether faulty parts or incorrect assembly have undermined the basic designed-in safety features.

Clearly, the traditional approach taken by the EMC testing community (domestic, commercial, industrial, automotive, rail, marine, aerospace, medical or military) is quite different from the approach taken by the safety community. A number of reasons why traditional EMC testing methods are inadequate (on their own) for ensuring functional safety follow.

Immunity Testing Only Covers One EM Disturbance At A Time

In real life and normal operation equipment is subjected to a number of electromagnetic disturbances simultaneously, for example: radiated fields from two or more transmitters simultaneously transmitting; a continuous radiated field plus a fast transient burst or electrostatic discharge; etc.

In many cases the problem seems to be that, for example, one of the EM disturbances "uses up" most of the noise margin in a digital system, so that when a simultaneous disturbance occurs even a very low level can cause a malfunction.

However, simultaneous radio-frequency disturbances can cause more exotic and unexpected interference problems, by intermodulating within electronic devices. The resulting problems may be reasonably foreseeable (to someone who is aware of the possibility) but might not be tested by traditional EMC tests.

Michel Mardiguian [7] has shown that when one EM disturbance is applied (e.g. a radiated RF field) the immunity of the equipment to another disturbance (e.g. fast transient bursts) can be seriously compromised.

In his conclusions he stated: "Speculating that all the worst EMI threats will appear at the same time on a given system would be extravagant. But relying on the belief that certain EMI combinations will never exist could be just as imprudent. Crude modeling, and a series of three simple tests are suggesting that within the frame of what has been simulated, the combination of effects is a real risk....for those applications where combined threats could happen, the product specification or the test plan should require a greater EMC margin, to cover a possible simultaneous exposure."

Immunity Tests Do Not Simulate Real-Life Exposure

EMC test methods are designed for accuracy, repeatability, and low cost – and may not simulate real life very well. For example: most radiated EM field immunity testing is done in anechoic chambers that create an environment unlike every real-life situation (apart from that of an aircraft or missile in free flight). In real life there will be one or more surfaces reflecting EM fields onto the equipment from a variety of angles.

The waveforms used for fast transient burst, surge and electrostatic discharge testing can be very simplified versions of the real-world EM disturbances they are supposed to represent. In some cases the test waveforms are defined by what test equipment can be manufactured at an affordable price. For example, fast transient burst (FTB) testing uses pulses with fixed amplitudes and a repetition rate of 5kHz, whereas the EM disturbances from the electro-mechanical contacts that the FTB test is intended to represent actually varies in frequency from MHz to kHz as the contact gap opens, with an amplitude that rises as its frequency decreases.

Immunity test methods are often too simplistic. For example, electronic warfare and munitions EMC experts know that when an RF 'threat' is modulated at a frequency corresponding to the rate of electrical or software activity in the target equipment, the susceptibility vulnerability of the target increases dramatically. Real world sources of RF interference have a huge possible range of modulation frequencies, but normal immunity testing (using IEC/EN 61000-4-3 and IEC/EN 61000-4-6) uses only a 1kHz modulation frequency, so does not indicate the response of the tested equipment to real-life RF threats.

The latest version of the medical equipment safety standard IEC/EN 60601-1-2 employs an additional modulation frequency of 0.5Hz for equipment that monitors physiological parameters, but this is still insufficient.

[8] makes the point that normal testing standards can give an erroneous impression of an equipment's EM performance in real life, due to the effects of load and temperature variations upon the inductors used in EMI filters. EMC testing standards usually test at just one setting of the equipment's load – but it is well known that the levels of current flowing in the inductors of a filter will alter their inductance values due to variations in permeability (and even saturation). EMC testing standards also test at just the nominal value of the mains voltage – whereas higher or lower voltages will alter the currents in the supply filters' inductors and thereby alter their inductance values. Also, EMC testing standards only test at one ambient temperature – but it is well known that the inductance of an inductor varies with temperature.

Inductance variations due to current and temperature will alter the characteristics of the filter the inductor is used in, affecting the emissions and immunity of the equipment. [D] gives the example of a variable-speed motor drive tested for emissions to IEC 61800-3, at 25°C and 230Vrms with a light load on the motor. When retested at 40°C, +10% supply voltage, and full load the emissions from the variable speed drive were measured to be 20dB higher, indicating that the equip-ment's supply filter's performance had fallen by 20dB.

EMC "Risk Analysis" Is Not Done

Most immunity tests are based on the generic EMC standards (IEC/EN 61000-6-1 and -2, which replace the old EN 500821 and -2). These aim to cover the 'normal' EM environment but in fact have many shortcomings, for instance they do not cover the close proximity of cellphones even though this is a fact of life these days. They also only have surge requirements on the mains supply up to ±2kV when it is also a fact of life that normal single-phase mains supplies can expect a number of surges at up to ±6kV each year. A number of other failures to cover the typical modern EM environment could also be listed, but the standards make no attempt to cover low-probability EM disturbances.

Sometimes safety test standards, such as the medical device safety standard EN 60601-1-2, increase the frequency range that is covered during some immunity tests, and sometimes they increase the test levels (doubling the test level is a particular favorite). But good safety engineering practice requires a hazard assessment and risk analysis that includes an assessment of the reasonably foreseeable environment and the possible effects it could have on the equipment, and this is good safety engineering practice for the EM environment too.

At the moment this type of assessment is only required by IEC/TS 61000-1-2:2001 [5], but this is only a Technical Specification and could take years to become a full IEC standard, maybe even longer to be adopted as an EN and listed under EU safety directives.

This means that normal EMC immunity tests based on the generic standards cannot give any confidence that the tested example of equipment would be safe enough in its actual operating EM environment.

The IEC Advisory Committee on Safety (ACOS) Workshop VII, 9/10 March 2004, Frankfurt am Main, Germany heard from Simon Brown and Bill Radasky that: "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.” [9].

Immunity Testing “Compatibility Levels” May Be Too Relaxed

Each type of EM disturbance phenomenon varies according to some statistical parameters. The question arises of where to set the pass/fail level for an immunity test, within this statistical variation. This level is known as the “Compatibility Level”, and it is often set at the two-sigma level (sigma being the standard deviation).

This level means that 95% of the population of events of this type of disturbance can be expected to fall below the test level. But it means that 5% of disturbances (one out of every twenty) can be expected to be higher than the test level.

Whilst the two-sigma level may be a suitable compromise between performance and cost for domestic, commercial and industrial products and equipment which have no impact on safety, a one-in-twenty chance of malfunction or failure upon exposure to some EM disturbances could be unacceptable where there could be safety implications, especially where the Safety Integrity Level (SIL) requirements according to IEC 61508 [4] are high.

Foreseeable Faults Are Not Addressed By Immunity Testing

When considering the EMC requirements for achieving adequate levels of functional safety, there is an understandable tendency to focus on more extreme or unusual EM disturbances, which usually have a low probability. But commonplace electrical faults can significantly affect the susceptibility to the normal levels of EM disturbances in equipments’ environments, causing unreliable operation.

Here are some foreseeable faults that can ruin equipment’s immunity to its normal EM environment.

- Dry joints or short circuits (e.g. in a filter)
- Out-of-tolerance components that could affect EM performance (e.g. by making feedback amplifiers less stable)
- Loose fixings in enclosure or cable shielding assemblies
- Conductive gaskets missing or damaged during assembly
- Failure of a surge protective device
- Unknown use of a ‘die-shrunk’ integrated circuit (can have markedly different EMC characteristics to the normal part, although sold under the same part number with no distinguishing marks)
- Incorrect values of EMC-related components fitted by mistake

Safety validation traditionally considers foreseeable faults (e.g. shorted or open-circuited components) to check that the equipment remains safe (e.g. “single-fault safety”). But no one has ever done EMC immunity testing in a similar way – retesting the EM performance after simulating each foreseeable fault in turn.

Since traditional EMC testing methods do not take account of any faults, as safety validation must, they are unsuitable as a sole means of verifying EMI-related safety performance. In the author’s view, this shortcoming is sufficient, on its own, to show that the normal approach to EMC is completely inadequate (on its own) where interference could lead to undesirable safety consequences.

Effects Of The Physical Environment On EM Performance

For adequate safety performance to be maintained over the lifecycle of an equipment, the minimum EM performance required must be maintained despite the effects of its physical environment. These effects can be assessed as immediate, or long-term (ageing).

Shock and vibration, temperature extremes and temperature cycling, can have an immediate bad effect on EM performance – for example by causing poor electrical contact at joints and gaskets and thereby reducing the effectiveness of filtering or shielding. Also, installing an item of equipment in non-ideal situations commonly experienced in real life can twist or deform its structure and cause shield joints to open up slightly. But (apart from IEC/TS 61000-1-2) no non-military EMC or safety standards cover this issue.

An equipment's lifetime exposure to its physical environment, including climatic conditions such as condensation and weathering, and issues such as salt spray, mould growth, sand and dust, cleaning solvents and spillages – plus wear and tear caused by multiple operations of controls and the opening and closing of doors and access panels – all contributes to what we call "ageing". The inevitable corrosion at metal joints is known to degrade EM filtering and shielding performance and cause immunity to worsen as equipment ages. Ageing has never been observed to improve EM performance – it always degrades it.

But normal EMC testing is applied only to pristine new items, in a benign environment, and never covers the possible effects of the physical environment or ageing. So although adequate safety performance must be maintained for many years, the EMC-related functional safety performance aspects of an item of equipment upon exposure to its normal physical environment, after a few years of life, remains unknown.

[10] concludes that: "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."

Only A Representative Sample Is Tested For EMC

Most companies design their equipment, test it using 'black box' EMC test methods, then modify it as required until it passes its EMC tests. But most of them have no real idea whether the final version passed because of good design, or because of a fluke that might not be repeated in future manufacture.

Maybe an altered cable routing or a different batch of ICs would make the EMC performance worse? Many companies introduce "small" changes in production, software "bug fixes", and substitute components – without re-qualifying EMC – and many don't routinely test EMC in serial manufacture either, so they have no real knowledge of the actual EM performance of the items of equipment they supply to their customers.

This should be compared with the approach typical of safety standards, which require testing of the basic safety features of every item of equipment manufactured, and a pass result documented for every item supplied to a customer.

The fact that an item of equipment once passed an EMC immunity test proves nothing at all about the quality of its EM design, or the EM immunity performance of the items actually supplied.

EMC Testing Does Not Address Maintenance, Repair, Refurbishment, Upgrades (e.g. software)

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 no EMC testing standards do.

Performance Degradations Acceptable For EMC Might Not Be Acceptable For Safety

It is often difficult to test a system in-situ, so tests on individual items of equipment or system sub-assemblies is often considered adequate instead. But a simple example will show that this can lead to great problems.

It is usually considered perfectly acceptable for as 24Vdc power supply unit to meet Performance Criterion B during a FTB test (using IEC 61000-4-4 as the basic test method), because this is permitted by the generic immunity standards. Criterion B permits any amount of momentary degradation during the test as along as the equipment self-recovers to normal operation immediately after the test. For some power supplies, the FTB test causes semiconductor protection measures to operate and their output collapses quickly to 0V during each burst.

But in a system this 24Vdc power supply might be powering a single-board computer or programmable logic controller (PLC) and the complete removal of its 24V supply would almost certainly cause it to reboot, so that after the test it would not immediately self-recover to its original state. In fact it might not self-recover at all and manual intervention might be required.

Where a continuous safety function is required from the system comprising the 24Vdc power supply and computer board or PLC, it would have to continue to work as normal during and after the FTB test. Where an "on-demand" safety function was required from the system, it might be permitted for it to "crash" and recover within a few seconds – depending on the SIL level and probability of the FTB events. But it is almost certain that no safety system would ever be permitted to require manual intervention after such a commonplace EM disturbance.

This simple 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.

[9] 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."

Conclusions

EMI-related aspects of functional safety cannot be verified by normal EMC test methods. Indeed, if it was possible to devise an EMC immunity test regime that correctly addressed all of the above issues – it would cost more, and take longer, than any manufacturer could possibly afford.

[9] says: "EM immunity testing alone (even at higher levels than normally applied or EMC testing) does not give the necessary confidence that equipment is acceptable, for use in a safety application."

Instead, to reduce the safety risks which could be caused by EMI, methods similar to those already employed for all other safety issues should be employed – the application of well-proven and well-understood EM assessment, design and assembly techniques, backed up by a suitable program of EMC testing that verifies the suitability of the techniques used.

These EMC good-engineering-practice techniques should aim to ensure that the level of confidence that equipment will work correctly – for the equipment's lifetime, electromagnetic, physical and climatic environments, reasonably foreseeable use and single faults – is not likely to be compromised by EMI. 'Black box' EMC testing, the method currently employed, cannot possibly achieve this goal.

This same situation has already been met with safety-related software. It is totally impractical to prove such software is safe by testing it – it would cost more, and take longer, than any manufacturer could possibly afford. However, over recent years software experts world-wide have devised and validated design methods, the use of that will achieve whatever levels of safety integrity are required [11]. It is now time to do the same for EMC. ■

References

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

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

[3] New guidance on EMC and Safety for machinery, Keith Armstrong, 2002 IEEE International EMC Symposium, Minneapolis, August 19 - 23. Conference Proceedings: ISBN: 0-7803-7264-6, pp. 680-685.

[4] EMC for Functional Safety, IEE (London, UK) training course (first held February 10th 2004), http://www.iee.org.uk/.

[5] 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.

[6] Review of Progress with EMC-Related Functional Safety, Keith Armstrong, 2003 IEEE EMC Symposium, Boston, August 18-22 2003, paper presented in Open Forum 3 on August 20, CD-Rom;2003: ISBN 0-7803-7836-9; Softcover: ISBN 0-7803-7835-0

[7] Combined effects of several, simultaneous, EMI couplings, Michel Mardiguian, 2000 IEEE International Symposium on EMC, Washington D.C., August 21-25 2000, ISBN 0-7803-5680-2, pp. 181-184.

[8] EMC Performance of Drive Application Under Real Load Condition, F Beck and J Sroka, Schaffner EMV AG application note, 11th March 1999.

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

[10] The Case for Combining EMC and Environmental Testing, W H Parker, W Tustin and T Masone, ITEM 2002, www.rbitem.com, pp 54-60.

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

Acknowledgement

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

About The Author

Keith Armstrong, Partner of Cherry Clough Consultants, can be reached at keith.armstrong@cherryclough.com.