Another EMC resource
from EMC Standards

Design and Mitigation Techniques for EMC for Functional Safety

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

Design and Mitigation Techniques for EMC for Functional Safety

EurIng Keith Armstrong
Cherry Clough Consultants
Denshaw, U.K.

Abstract

Certain kinds of equipment must maintain sufficiently low risks to users and third parties over their entire lifecycles, despite at least one fault, and despite foreseeable misuse.

Where electromagnetic interference (EMI) could foreseeably have an effect on such equipment, it will need to maintain an adequate level of electromagnetic (EM) immunity over its lifecycle. This is the concern of 'electromagnetic compatibility (EMC) for Functional Safety'.

The EM environment that such equipment could experience over its whole lifecycle can be very different from that tested by standard 'EMC compliance' immunity tests. IEMI – Intentional EMI – could also be a concern.

The physical and climatic environments, plus the wear and tear and misuse that such equipment is subjected to over its lifecycle can cause circuit EM behavior to alter, and can degrade the performance of EM mitigation measures such as shielding and filtering.

It is not generally practical to prove that an equipment is safe enough – as far as EMI possibilities are concerned – solely by EMC testing. In all areas, including software, safety is achieved by the use of appropriate design techniques, plus testing, and this is also true for EMC for Functional Safety.

This paper briefly describes the EMC design techniques that help achieve an adequate level of safety. Appropriate testing techniques will be covered in a future paper.

Although this paper focuses on safety concerns, the design techniques it discusses are also important for high-reliability, mission-critical and legal metrology equipment, or to help control financial or security risks.

Introduction

A system that could have an impact on functional safety, or is 'safety-related' or 'safety critical', should maintain sufficiently low risks to users and third parties over its entire lifecycle. It is usually required to be safe despite the occurrence of at least one fault, and also despite foreseeable misuse. Nuclear electromagnetic pulse (NEMP or HEMP) or IEMI may be a concern in some applications.

In such a safety system, where foreseeable EMI could affect its electrical or electronic hardware or software during its operational lifetime and increase safety risks – the equipment concerned will need to maintain sufficient EM immunity over its lifetime.

This is an aspect of what is usually called 'EMC for Functional Safety' – a very different discipline from compliance with EMC immunity regulations, such as those in the European Union's EMC Directive. These differences were discussed in [1-5] and are not repeated here.

Safety must be achieved despite (at least) one fault, so any foreseeable faults must either result in a fail-safe situation (such as a safe shut-down) – or else must result in continued safe operation (i.e. the EM immunity performance must not fall below a certain level). Examples of faults that can affect immunity include the failure of a surge protection device; a broken filter ground connection, a badly assembled or damaged EMC gasket, etc.

The physical environment over the lifetime can degrade immunity performance, for example corrosion can cause shielding joints and filter ground bonds to become high resistance, ruining their EM performance. Shock and vibration, bending forces, temperature extremes or cycling, wear and tear and many other lifetime mechanical, physical and climatic influences can affect the radio-frequency stability of some types of circuits, and degrade shielding and filtering performance.

The EM performances measured by the normal 'EMC compliance' immunity tests are very poor indicators of an equipment's behavior in real life, for the reasons described in [6, 7]. An EMC test plan that covered all of the above issues and gave sufficient confidence would be impractical in the extreme – much too lengthy, and much too costly.

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 EMC testing.

IEC 61508 [8] is the basic IEC standard on Functional Safety, and applying it to our safety system tells us how to determine the SILs (Safety Integrity Levels) we need for its 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 test the EMC performance. A suitable procedure is as follows:

a) Determine the worst-case EM, mechanical, physical, climatic and biological environments that the equipment will be exposed to during its lifetime. This was described in [9] and is not repeated here.

Presented at the IEEE 2006 International EMC Symposium, Portland OR, Aug 14-18 2006

b) Create an environmental specification for the equipment, which will serve as the basis for the 'EM design specification' and the 'EM test specification'.

c) Specify the performance criteria that the equipment's functions should achieve when exposed to the worst-case EM phenomena in its environment.

d) Design so that the equipment will shut safely down or else maintain sufficient levels of immunity despite the lifetime effects of its environment. The degree of confidence required depends upon the SIL rating for the safety function – so the higher the SIL, the more diligence should be applied to design.

e) Test to verify the relevant aspects of the EMC design, and to gain confidence that the equipment is immune enough for its environment.

The rest of this paper discusses items b), c) and d) above. Item e) will be the subject of a future paper.

Never rely solely on standards

MIL-STD-464 says: "There is no substitute for a well thought out criteria for a system based on its operational requirements", and this is true for everything from toasters to railway trains. Competent engineers must carefully assess every equipment with respect to its operational situation(s), no EMC or safety standard can ever be relied upon to specify *exactly* what is required.

Specifying the levels in the EM design specification

There are inherent uncertainties in…

- The assessments of the worst-case lifecycle EM, mechanical, physical, climatic and biological environments
- The test levels that will actually be applied during immunity testing
- The performance of individual units in serial manufacture (due to component tolerances, uncontrolled variations in assembly and installation, etc.)

Because of these uncertainties, the worst-case exposure levels determined as described in [9] need to be increased by carefully chosen 'margins' before they are put in the EM design specification. The higher the SIL, the more confidence is required, so the greater the margin. For example: MIL-STD-464 employs a margin of 6dB for safety-critical and mission-critical equipment, and a 16.5dB margin for ordnance (bombs, missiles, etc.), to cope with the uncertainties associated with these two types of equipment.

EMC test levels are not a function of the SIL rating. Whatever the SIL, the worst-case EM 'threats' will be experienced from time-to-time during the lifecycle. Instead, SIL is concerned with the likelihood of unsafe failure *when* those worst-case EM threats occur.

So when creating the EMC design and EMC test specifications, an analysis of the various uncertainties is required, and the specified exposure levels increased by the appropriate 'margins', for each cell in the threat/function matrix (below).

An EM threat example…

- Uncertainty in assessment of worst-case lifecycle radiated field: ±6dB (for example)
- Uncertainty in radiated immunity test level: ±5dB (for example)
- Variations in unit EM performance due to tolerances, etc: ±4dB (for example)

We might decide that for the safety functions in SIL1 and SIL2 safety systems, the margin can be determined by 'root-sum-squaring' the independent variables, in this example giving us a margin of 9.4dB.

However, for SIL 3 or SIL 4 systems, which are usually ones which, if they malfunction, can cause large loss of life, we might choose to cover the unlikely event that the three independent uncertainties above all take worst-case values at the same time, in which case the margin would need to be 15dB.

Specifying the functional performance criteria

Before the design can begin, it is necessary to specify the performance criteria that the equipment's functions should achieve when it is exposed to its worst-case foreseeable EM phenomena. So the EM design specification usually takes the form of a matrix of EM 'threats' versus functions – with the performance required specified in each of the resulting cells. The performance criteria B and C in the normal IEC and EN immunity tests have no place here, we must know *exactly* how the equipment behaves when interfered with.

Function / EM threat	Actuator position error	Pressure error	Warning siren
100V/m 27MHz - 18GHz	< ±0.1mm during / after test	< ±0.1% during / after test	Must *not* operate when *not* required, or fail when required
400V/m 800MHz - 5GHz	< ±1mm during / after test	< ±1% during / after test	Must *not* operate when *not* required, or fail when required
1kV/m 2.35 -2.55GHz	< ±1mm during /after test or fail-safe	< ±1% during /after test or fail-safe	May operate when not required, must not fail when required
Line-to-ground damped oscillatory wave up to ±6kV	< ±1mm during /after test	< ±1% during /after test	May operate < 1s upon each surge, must not fail when required
Etc…	Etc..	Etc..	Etc..

Figure 1 Example of a threat / function matrix

Now that we have created our EM design specification we can begin our design. Remember that IEC 61508 specifies the use of certain design techniques for both hardware and software, and that these will depend upon the SIL.

Determining the 'natural' susceptibilities of hardware and software

An EM phenomena at any frequency can interfere with hardware or software if its level is high enough – but all hardware and software is especially vulnerable (maybe as much as 40dB more) at certain frequencies, related to resonances in its

structures, circuits or loads; or to the rates at which certain electrical operation occur, such as a digital system's clock frequency and its harmonics. An equipment's vulnerable frequencies are its major limiting factors for immunity, so knowing what they are helps the EM design.

We can determine the natural frequencies at which hardware and software are especially susceptible by analyzing, simulating, or testing the equipment without any EM mitigation measures applied to it.

When the especially susceptible frequencies are known, we need to decide whether they can occur – with significant levels – over the lifetime of the safety system. Direct interference, demodulation, and intermodulation should all be taken into account.

For example, if a circuit is especially susceptible to 1MHz, it might seem that using shielding and filtering effective at 1MHz can easily protect against this frequency. But if a potentially interfering signal at 2.450 GHz present in the environment is modulated at 1MHz, or if it is present at the same time as another signal at 2.451 GHz, each will easily pass through the 1MHz mitigation measures – and then either demodulate or intermodulate inside the circuit itself to create internal interference at 1MHz.

Analysis of especially susceptible frequencies, and of how the environment can cause them to appear in the circuits, helps cost-effective design by revealing which areas need the most design effort.

Fault mitigation

Faults can include…

- Components open/short circuited, or their parameters altered
- Broken electrical bonds (e.g. shield joints and gaskets, filter grounding)
- Increased impedance of electrical bonds

The use of design techniques that protect against the effects of the foreseeable physical (mechanical, climatic, etc.) environment can reduce likelihood of most systematic faults to low enough levels. HALT (highly accelerated life testing) can be used to help identify design shortcomings.

Random failures can still occur, and if they can lead to a safety risk IEC 61508 specifies design techniques for achieving the required SIL (e.g. duplication, triplication, etc.; automatic condition monitoring with safety shut-down; etc.).

EMI mitigation for multiple redundant channels

EMC is a systematic ('common cause') failure, so, where IEC 61508 requires multiple channels – with electronic voting on their results – to meet the SIL it is necessary to use diverse (different) technologies, so that all of the channels do not fail in the same way at the same time and defeat the purpose of the voting circuit.

But using multiple diverse technology channels does not necessarily mean that each channel can be allowed to have a low EM performance – otherwise, during interference, it could happen that all of the digital channel outputs were at 0 or 1, and all the analogue channels could be at plus or minus full scale. In such situations the chances of defeating the voting circuit can be relatively high.

One way around this problem without increasing the immunity of the channels could be send complex digital or analogue signals (such as a pulse train with specified timings) to the voting circuit instead of simple voltage levels. A failed channel would not create the complex signal and the (more complex) voting circuit would not be so easily fooled.

Similar 'common-cause' issues exist for some physical threats (e.g. overtemperature), with similar results.

Interference sensing techniques

Interference sensors can be used inside or outside equipment, to detect EM events which might cause hazards and initiate special protective measures or shut-down the equipment safely. For example:

- As already used to protect some military equipment from the pulses caused by nuclear explosions
- As already used by gaming machine manufacturers to protect from people trying to 'break' the machine with interference (e.g. 30kV ESD from cattle prods)

A safety interlock on a door or panel can tell if it has been opened, and inhibit the equipment so as to protect from the possible safety consequences of degraded shielding (treating the shielded door like a machine guard that interlocks with an emergency stop function).

There are also wideband EM sensors that can detect accidentally degraded shielding or filtering, or unforeseen EM threats, and initiate a safe shut-down. If these are used inside a shielded enclosure they could allow doors and panels to be opened without a safe shut-down occurring – unless EM threats are present at levels that could cause interference.

Don't rely too much on fail-safe methods

The user or operator will become very frustrated if a safety system initiates a safe shut-down every time the EM environment gets a little noisier than usual. It is not unusual for people to modify such safety systems, so that they can reduce costly downtime.

Because it is reasonably foreseeable that people will disable safety systems that cause excessive downtime, this counts as foreseeable misuse and an organization could be held to be liable for not taking it into account during design.

'Layering' mitigation

There are a number of design techniques that can produce hardware and software that is inherently more immune to EM phenomena. Alternatively, sufficient immunity achieved using only EM 'mitigation measures', such as filtering, shielding, surge suppression, etc. See [10 - 18] for more information on EMC design and mitigation techniques for hardware, and [10, 19 - 24] for more information on software EMC design techniques.

It can be easier, less costly, and more reliable, to use a number of 'layers' of inherent EM performance and EM mitigation measures, rather than relying on a single layer (such as a single equipment enclosure employing high-performance shielding and filtering).

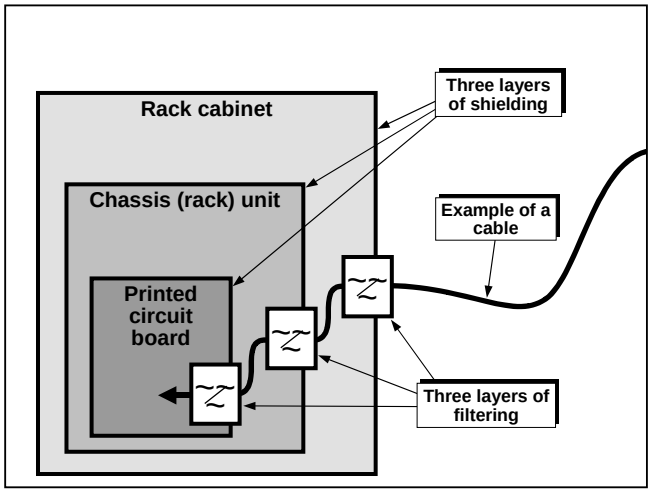

Figure 2 An example of 'layered' EM design

It is recommended to design so that if one 'layer' should fail completely for some unforeseen reason (e.g. misuse, whether accidental or intentional) – the equipment will still have at least adequate EM performance.

For example: assume that an enclosure requires a minimum of 40dB shielding effectiveness (SE) at 900MHz. A single shielded/filtered enclosure could easily achieve an SE of 80dB or more at 900MHz, and such enclosures are available from numerous suppliers. But cutting a single hole just 15mm in diameter (e.g. to add an indicator lamp) would reduce its SE to around 20dB at 900MHz.

However, if a three-layer design were used instead, each layer of shielding/filtering achieving 20dB at 900MHz – even completely destroying the outermost layer would still leave the overall design with an SE of 40dB.

Layers that can benefit from improvements in their inherent EM performance include…

- Integrated circuits (ASIC, FPGA, custom, etc.) can be designed or chosen for good EM performance
- Electrical and electronic circuits, interconnections, printed circuit boards (PCBs) and software, can each be designed to have improved EM performance

Layers where EMC mitigation measures (shielding; filtering; surge, transient, ESD protection, etc.) can be applied include...

- Individual Integrated Circuits (ICs) or transistors on a printed-circuit board (PCB)
- An area of a PCB
- A complete PCB
- Modules and sub-assemblies
- Units (e.g. a rack mounting chassis unit)
- The overall enclosure level (e.g. rack cabinets)
- Vehicles, rooms, buildings and sites

Radio receivers are easily interfered with. Even very well designed receivers are very sensitive to EM threats in their RF 'channel', whereas poorly designed receivers can be susceptible over a much wider frequency range due to overload and intermodulation in their RF stages. Digital signals with error-correcting protocols can help make radio communications more robust, and spread-spectrum techniques can be designed to resist all but very broadband interference.

MIL-STD-464 describes how multiple transmitting / receiving antennas can be co-located, and identifies simulators that can help designers to avoid problems.

All interconnections are weak points

Fiber-optics and wireless data communications are preferred to metallic cables for signal, data and control. Data in metallic cables should be protected by a proven error-correcting protocol (e.g. MIL-STD-1553). But all interconnections can be affected by EM and/or physical threats, so failure detection with automatic switching to a reserve connection with a different route may be required, or safe shut-down.

Don't rely on the user

It can sometimes be tempting to try to arrange for your customer to bear the cost of some EM mitigation measures, by adding them to the user manual. The assumption might be that it will be the customer's fault if a safety incident occurred because he did not read and fully implement the requirements in your manual.

But this approach might not provide a good legal defense – because everyone knows that no one reads manuals, and yet safety must still be achieved even considering reasonably foreseeable use or misuse.

So, when relying on mitigation at site-level for the safety of your system, always agree it in writing well beforehand with the customer, and maybe agree site verification requirements too so you can check that he has done it correctly. It is important to include an agreed legal disclaimer that has the effect of making the customer solely liable if the site improvements are not fully implemented before a safety system is operated.

Designing to prevent the physical environment from causing EMI

The equipment must be designed so that its EM performance remains sufficient despite all foreseeable physical stresses, wear and ageing. Mechanical structures may need to be designed for foreseeable worst-case forces, shock and vibration with the aid of finite element analysis.

Physical mitigation techniques include: shock and vibration mountings (active or passive); vibration-proof fixings; encapsulation; grease; paint; cable ties; anti-condensation heaters; sealed enclosures; forced ventilation; air-conditioned enclosures, etc.

Just as for EM performance, using two or more 'layers' of

physical protection can cost less and be more reliable than relying on a single layer, and can be less vulnerable to unforeseen circumstances, failures and misuse (whether accidental or intentional).

EMC problems caused by foreseeable use (misuse)

Installation, commissioning or maintenance instructions might not be followed, so it is best if the manufacturer does these tasks. Users might open doors, covers or panels when they should not, or make unapproved modifications – so the designer needs to anticipate what could foreseeably happen, then design, guard and warn accordingly (in that order). Sometimes users will need to be trained, maybe even pass an exam, before being appointed as a "keyholder".

Control of the build-state is vital

All of the following can be EMC-critical:

- A single 'form, fit and function' replacement part
- A wire or cable routed differently
- IC and semiconductor mask-shrinks (die-shrinks)
- 'Latest generation' power semiconductors
- Changes in painting method or supplier (e.g. overspray where electrical contact is required)
- Changes in metal suppliers (e.g. non-conductive passivation automatically applied)
- Metal fixings supplied with non-conductive finishes
- Almost any design or component changes made by electronic unit or sub-assembly suppliers – the build-state of their goods should also be controlled

So, design change-control EMC procedures are required. The QC system should ensure that no changes in any aspect of build-state can occur — however insignificant they may appear — unless checked and approved by the company's EMC authority. EMC 'checks' or full retesting, may be required before the change or deviation can be authorized.

Similar considerations apply to controlling the design to withstand the foreseeable physical environment.

Systems and Installations

A number of design techniques exist for helping to achieve the desired EMC in systems and installations, including cable segregation and routing, provision of paths for the return of common-mode currents, and the 'mesh' bonding of the earth/ground structure. These also help in the application of the usual EM mitigation techniques (filtering, shielding, transient/surge suppression, galvanic isolation, etc.), see [14] and [15] for details.

Control of suppliers and subcontractors

Some companies find it difficult to achieve the necessary degree of control over suppliers and subcontractors, so to reduce their risks they use...

- Sample-based EMC checks upon delivery (these can be quick and easy to do if designed correctly)
- Sample-based EMC tests in serial manufacture (frequent quick checks, with full tests every few months)

Good manuals are a mitigation technique too

Carefully written manuals are required to help achieve safety in real life, and to try to limit liability in the case of safety incident. They should clearly describe all that should be done so that the safety system really is as safe as it should be – for its whole lifecycle. They should always include a legal disclaimer that makes the customer liable if the instructions in the manuals are not followed exactly.

Maintenance

Overcurrent and overvoltage protection devices often have a limited effective life, which depends on the EM environment they are exposed to. Where their failure could increase safety risks, planned maintenance should check and replace them as necessary before they fail. Planned maintenance may also be required to check and repair cable shields and terminations, gaskets, filters, RF bonds, galvanic isolation, misuse, damage, unapproved modification, etc.

Cost-effective maintenance benefits from designing-in appropriate test features, to help maintain EM performance over the lifecycle (e.g. providing diagnostic test points at external connectors). It is increasingly practical for equipment to test itself, log faults, etc., and report its status via cellphone networks or the Internet, so that maintenance visits only occur when necessary.

Maintaining EM performance despite repairs, maintenance, refurbishment

Maintaining EMC post-manufacture is made much easier if all the EMC-critical elements of a design or equipment are shown on the drawings, or identified in their part numbers. So it should be part of the design process to identify all of the 'EMC-critical elements', marking-up drawings and raising new part numbers accordingly.

Maintenance and repair should not alter any 'EMC-critical elements' of the build state, even down to very tiny details, and should use exactly the same EMC-critical parts, assembly methods and processes, as the original. Some gaskets may need to be checked and replaced, and all of the fixings must be refitted with their correct torques. Partial or full EM testing may be required afterwards, to ensure EM performance has not been compromised.

The general rule is — "Do not design it if it cannot be repaired", and this is good advice for equipment that is large, has a high-value, or is permanently installed. But some household appliances, consumer goods, high-volume or low-cost products are intended never to be maintained, and their functional safety design can be more challenging – especially because large numbers of people could be exposed to the risks of their hazards at any one time.

Independent reviews

Companies and institutions (e.g. universities, training organi-

zations) can have corporate cultures that include bad or non-ideal practices, or what we might call 'blind spots', but they generally cannot detect them in themselves. So, independent reviews of EMC design are recommended (especially for systems with high SILs). Even if the reviewers are not as expert as the designers, their different perspectives will help detect problems caused by cultural (institutional) issues.

References

[1] "Guidance on EMC and Functional Safety", IEE, 2000, http://www.iee.org/Policy/Areas/Emc/index.cfm

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

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

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

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

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

[7] "Functional safety requires much more than EMC testing", Keith Armstrong, EMC-Europe 2004 (International Symposium on EMC), Eindhoven, The Netherlands, 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] "Specifying Lifecycle Electromagnetic and Physical Environments – to Help Design and Test for EMC for Functional Safety", Keith Armstrong, 2005 IEEE International Symposium on EMC, Chicago, Aug 8-12, ISBN: 0-7803-9380-5, pp 495-499

[10] "Robust Electronic Design Reference Book, Volumes I and II", John R Barnes, Kluwer Academic Publishers, 2004, ISBN: 1-4020-7739-4

[11] "Design Techniques for EMC" Keith Armstrong, EMC Compliance Journal, 1999 and 2006 versions, www.compliance-club.com/KeithArmstrongPortfolio

[12] "Advanced PCB Design Techniques for EMC" Keith Armstrong, EMC Compliance Journal, 2005, www.compliance-club.com/KeithArmstrongPortfolio

[13] "EMC for Product Designers, 3rd edition" Tim Williams, Newnes, 2001 ISBN 0-7506-4930-5

[14] "EMC for Systems and Installations" Tim Williams and Keith Armstrong, Newnes 2000, ISBN 0-7506-4167-3

[15] "EMC for Systems and Installations" Keith Armstrong, EMC Compliance Journal, 1999, www.compliance-club.com/KeithArmstrongPortfolio

[16] "The Design of Military Equipment Enclosures to Minimise the Effects of Corrosion", John Terry, EMC-UK 2005 Conference, Newbury, Oct 13-14, pp 85-88

[17] "EMC and Electrical Safety Design Manuals", York EMC Services, 2002, sales@yorkemc.co.uk, phone: +44 (0)1904 434 440

[18] IEC 61805-3: "Functional safety of electrical, electronic and programmable electronic safety-related systems – Software Requirements"

[19] "Noise, EMC and Real-Time", MISRA Report 3, February 95. The Motor Industries Software Reliability Association (MISRA), http://www.misra.org.uk

[20] "Electromagnetic Compatibility of Software", IEE Colloquium, Thursday 12th November 98, IEE Colloquium Digest: 98/471, sales@iee.org.uk

[21] "EMC-Hardening Microprocessor-Based Systems" Dr D R Coulson, IEE Colloquium "Achieving Electromagnetic Compatibility: Accident or Design", 16th April 97, IEE Colloquium Digest: 97/110, sales@iee.org.uk

NOTE: The software techniques described in the three references below are equally valuable for improving software immunity to all transients, the main causes of EMC problems for software

[22] John R Barnes, "Designing Electronic Equipment for ESD Immunity", Printed Circuit Design, vol. 18 no. 7, July 2001, pp. 18-26, http://www.dbicorporation.com/esd-art1.htm

[23] John R Barnes, "Designing Electronic Equipment for ESD Immunity Part II", Printed Circuit Design, Nov. 2001, http://www.dbicorporation.com/esd-art2.htm

[24] John R Barnes, "Designing Electronic Systems for ESD Immunity", Conformity, Vol. 8 No. 1, February 2003, pp. 18-27, http://www.conformity.com/0302designing.pdf