Another EMC resource
from EMC Standards

Tutorial on EMC for Functional Safety part 2

Helping you solve your EMC problems

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

Emc4fs-2.5B CCC

EMC mitigation techniques for Functional Safety

Cherry Clough Consultants

www.cherryclough.com

Eur Ing Keith Armstrong CEng MIEE MIEEE ACGI
phone: +44 (0)1457 871 605 fax: +44 (0)1457 820 145
keith.armstrong@cherryclough.com

Emc4fs-2.5B CCC

Contents of this module

Emc4fs-2.5B CCC

The 'worst-case' EM environment(s) must be assessed, including low-probability threats

- To help create the design and test specifications for a safety system
- All EM environment assessments require competent expertise
  - and some can require site surveys
- EM environment assessment is not discussed further here (but see the references)

Emc4fs-2.5B CCC

The *physical* environment(s) must also be assessed – so that the EMC mitigation measures can be designed correctly

- E.g.…
  - air pressure extremes and cycling, humidity, temperature extremes and cycling, etc.
  - shock, vibration, mounting tolerances and forces, etc.
  - dust (conductive?), condensation, spray (salty?), etc.
  - exposure to fuel, solvents, acids, alkalis, etc.
  - wear/tear, maintenance, cleaning, ageing, etc.

Emc4fs-2.5B CCC

The *physical* environment continued...

- There are well-established IEC and military standards covering a wide range of physical environments, e.g.…
    - various types of storage and transport
    - various types of operational locations
  - with comprehensive data on their physical parameters
- But calculations and instrumented site surveys might also be required
  - for environments which differ from the standards

Emc4fs-2.5B CCC

Determining the EM performance criteria

- Different functional safety performance criteria will be required for the various safety functions
  - when they are interfered with by the various EM threats
- So it is necessary to create a matrix of safety functions versus EM threats
  - with the functional performance required specified in the resulting cells
    - note that the usual immunity test performance criteria (A, B and C) don't apply – we need to know <u>exactly</u> what happens when interference occurs

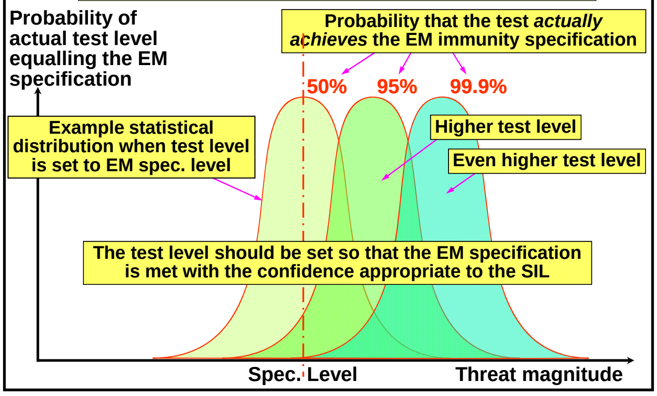
Emc4fs-2.5B CCC

Example of a threat / performance matrix

EM threat \ Function	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..

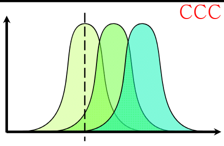
Emc4fs-2.5B CCC

Margins, SILs and confidence



Emc4fs-2.5B CCC

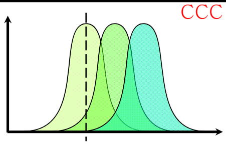
Margins, SILs and confidence
continued…



- All equipment will be exposed to worst-case environments during its lifetime
- So each physical or EM immunity specification should be based on the *worst-cases* of each type of threat
  - *regardless of the IEC 61508 'SIL' required*
  - taking foreseeable future changes in the physical or EM environments into account

Emc4fs-2.5B CCC

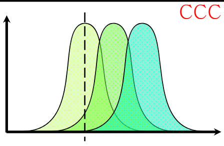
Margins, SILs and confidence
continued…



- There are inherent uncertainties in the…
  - a) Assessments of lifecycle EM & physical environments
  - b) Stresses actually applied during immunity tests
  - c) Performance of individual units (e.g. due to component tolerances, variations in assembly and installation, etc.)
  - e.g. MIL-STD-464 employs a 6dB margin for safety-critical and mission-critical equipment, and a 16.5dB margin for ordnance (missiles, bombs, etc.)

Emc4fs-2.5B CCC

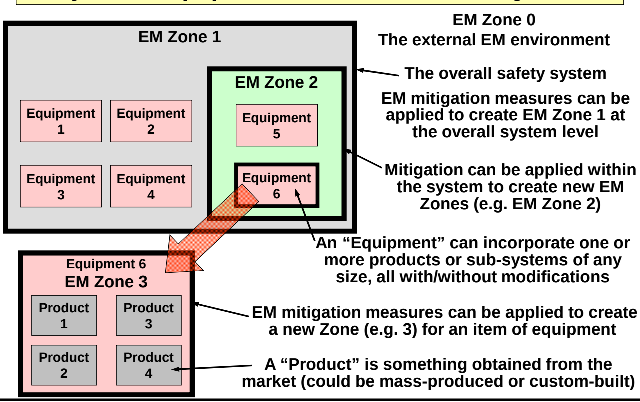
Margins, SILs and confidence
continued…



- So when setting the immunity specifications that will be used as the basis for the design, and for the verification tests
  - an analysis of the various uncertainties is required
  - and the specified threat levels increased accordingly by the resulting 'test margin'
  - for each cell of the threat/performance matrix (see earlier)
- A similar approach is required for physical stress tests

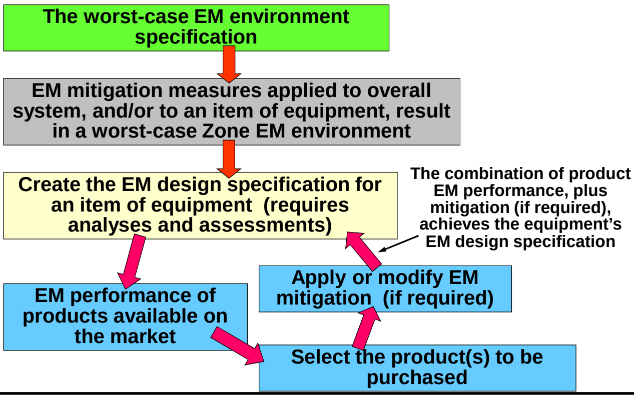
Emc4fs-2.5B CCC

System, Equipment, Products and Mitigation



Emc4fs-2.5B CCC

EM mitigation and the EM design specification



Emc4fs-2.5B CCC

Determining the 'especially susceptible frequencies' of hardware and software

- Equipment is *especially* susceptible at certain frequencies, including the…
  - full bandwidths of any analogue circuits
  - resonant frequencies of cables, metal structures, transducers or actuators
  - digital clock frequencies, sampling rates, RF carrier and modulation frequencies
    - and all of their harmonics

Emc4fs-2.5B CCC

Determining the 'especially susceptible frequencies' of hardware and software continued…

- So to achieve a cost-effective and safe design, it helps to analyse or test the effects of radiated and conducted RF on the equipment
  - *without any shielding or filtering fitted*
  - to discover its 'especially susceptible frequencies'
  - then determine how these frequencies ***could possibly*** be stimulated by the real operational EM environment over the lifetime
    - e.g. by direct interference, demodulation, intermodulation

Emc4fs-2.5B CCC

Determining the 'especially susceptible frequencies' of hardware and software continued…

- Intermodulation occurs in all semiconductors, and at all corroded electrical joints (known as the 'rusty bolt effect')
  - an important lifecycle consideration
    - (normal EMC RF testing uses single frequencies, so doesn't test intermodulation possibilities)
- To prevent demodulation and intermodulation from causing immunity problems in real life…
  - it may be necessary to shield and filter at frequencies well beyond the 'especially susceptible frequencies'

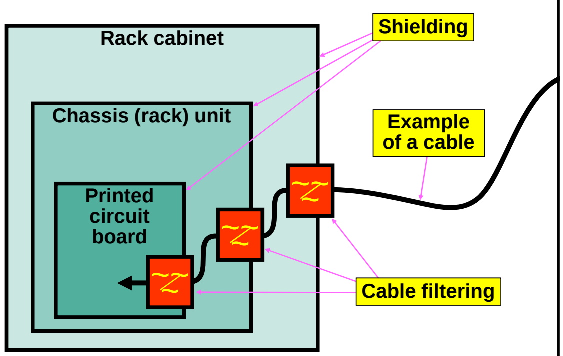
Emc4fs-2.5B CCC

A 'layered' approach to EM mitigation

- It is often less costly, and more reliable, to use a number of 'layers' of EM mitigation
  - rather than relying on a single 'layer'…
    - e.g. high-performance shielding and filtering of the equipment's enclosure
- 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 adequate EM performance

Emc4fs-2.5B CCC

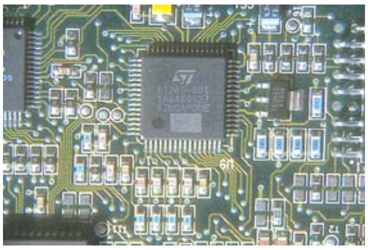
Example of 'layered' EM mitigation (using shielding and filtering)



Emc4fs-2.5B CCC

Layers

- **Integrated circuits (ASIC, FPGA, custom, etc.) can be designed or chosen for good EM performance**
- **Circuits, their interconnections and printed circuit boards can be designed for good EM performance**



Emc4fs-2.5B CCC

Layers continued...

- **Fibre-optic cables preferred for signal and control**
  - **or else cables should carry serial digital data protected by a proven robust error correcting protocol (e.g. '1553')**
- **Shielding; filtering; surge, transient, and ESD protection can be applied to...**
  - **individual devices**
  - **printed circuit assemblies**
  - **modules and sub-assemblies**
  - **units (e.g. rack mounted equipment)**
  - **overall enclosure level (e.g. rack cabinets)**
  - **and even to rooms, buildings, and sites (campuses)**

Emc4fs-2.5B CCC

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**
    - **e.g. used to protect some military equipment from the pulses caused by nuclear explosions**
    - **e.g. used by gaming machine manufacturers to protect them from people trying to 'break' the machine with interference (e.g. using cattle prods)**

Emc4fs-2.5B CCC

Interference sensing techniques continued...

- **A safety interlock on a door or panel can tell if it has been opened**
  - **and inhibit the equipment so as to protect people from the possible safety consequences of degraded shielding**
    - **treating the door like a machine guard that interlocks with an emergency stop function**
- **But EM sensors can detect *accidentally* degraded shielding or filtering, or *unforeseen* EM threats**
  - **and could allow doors to be opened *without protective* shut-down (unless EM threats are present)**

Emc4fs-2.5B CCC

EMC mitigation design techniques will not be described today

- **Refer to the references at the end of this module for shielding, filtering, suppression, isolation, etc.**
  - **for hardware, systems and installations, and software**

Emc4fs-2.5B CCC

Coping with foreseeable faults

- **Faults can include…**
  - **components open/short circuited, or altered parameters**
  - **broken electrical bonds (e.g. shield joints, filter grounding)**
  - **increased impedance at shield gaskets, etc.**
  - **appropriate design for the foreseeable physical environment can reduce likelihood of most faults**
- **Where a fault can lead to a safety risk, IEC 61508 describes design techniques for achieving the SIL**
  - **e.g. duplication, triplication, etc.**
  - **e.g. condition monitoring with safety shut-down, etc.**

Emc4fs-2.5B CCC

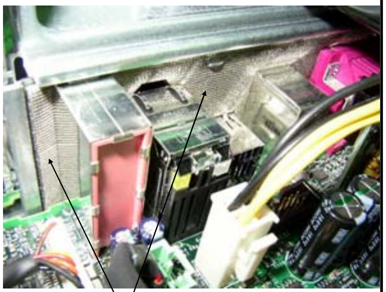
EMI mitigation when using multiple redundant channels

- EMC is a systematic (common cause) failure
  - so, where IEC 61508 requires multiple channels to meet the SIL, the use of diverse technologies is required
- But using multiple diverse-technology channels *doesn't mean* each can have low EM performance
  - otherwise, during interference, it could happen that *none* of the digital channels would function correctly
    - and all the analogue channels could be at + / - full scale
    - (a similar issue for common-cause *physical* threats)

Emc4fs-2.5B CCC

EMC problems which can be caused by the physical environment

- Static forces on a structure can make joints and gaskets open up
  - reducing shielding effectiveness

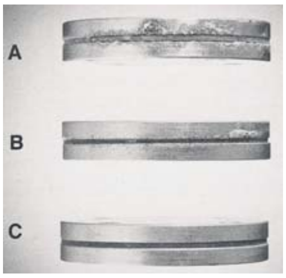


Shielding gaskets at the rear panel of a Dell Optiplex PC, 2002

Emc4fs-2.5B CCC

EMC problems caused by the physical environment continued...

- Repetitive stress, shock, vibration, oxidation and corrosion can cause…
  - wear-out of joints / gaskets
  - gaps in cable shields
  - loosened fixings
  - open / short circuits in conductors and component leads
  - connectors to work loose



Results of a test comparing lifetime corrosion for three different types of shielding gaskets

Emc4fs-2.5B CCC

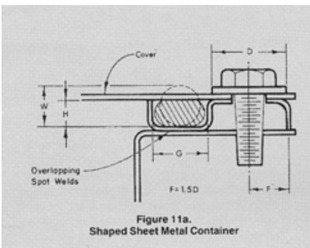
EMC problems caused by the physical environment continued...

- These physical effects can ruin shielding effectiveness
- They can also cause filters to become less effective
  - e.g. by breaking their ground connections
  - with similar problems for surge, transient and ESD protective devices
- And they can make circuits on PCBs unstable
  - much more prone to causing or suffering EMI

Emc4fs-2.5B CCC

Protecting from foreseeable "physical EMC problems"

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



Emc4fs-2.5B CCC

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

Underside view of an encapsulated filter

Emc4fs-2.5B CCC

EMC problems caused by foreseeable use (or misuse)

- Installation, commissioning or maintenance instructions might not be followed
  - so it is best if these tasks are done by the manufacturer
- Users might open doors, covers or panels when they shouldn't, or make unapproved modifications
  - so we must 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 a "keyholder"

Emc4fs-2.5B CCC

Self-diagnostics and automatic communications

- These techniques can be used to detect problems or misuse before they become serious
  - and automatically inform manufacturer
    - e.g. by email or GSM cellphone system
    - like vending machines that communicate their stock levels by GSM
- Manufacturers can send out appropriate personnel (e.g. repairer), with the right parts and tools
  - and/or warn user

Emc4fs-2.5B CCC

EMC mitigation techniques for Functional Safety

the end

Cherry Clough Consultants

www.cherryclough.com

Eur Ing Keith Armstrong CEng MIEE MIEEE ACGI
phone: +44 (0)1457 871 605 fax: +44 (0)1457 820 145
keith.armstrong@cherryclough.com

Emc4fs-2.5B CCC

Some useful references

- *Assessing an Electromagnetic Environment*
  Keith Armstrong, downloadable from the "Publications and Downloads" page at http://www.cherryclough.com
  - *Note:* this was written to help with EMC Directive compliance, not for safety purposes
- *The Case for Combining EMC and Environmental Testing*, W H Parker, W Tustin, T Masone, ITEM 2002 pp 54-59, www.rbitem.com
- *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
- *EMC Performance of Drive Application Under Real Load Condition"*, F Beck, J Sroka, Schaffner EMV AG application note, 11th March 1999
- *Robust Electronic Design Reference Book, Volumes I and II*, John R Barnes, Kluwer Academic Publishers, 2004, ISBN: 1-4020-7739-4

Emc4fs-2.5B CCC

Some useful references continued...

- *Design Techniques for EMC*
  Keith Armstrong, EMC Compliance Journal, 1999
  www.compliance-club.com/KeithArmstrongPortfolio
- *Advanced PCB Design Techniques for EMC*
  Keith Armstrong, EMC Compliance Journal, 2005
  www.compliance-club.com/KeithArmstrongPortfolio
- *EMC for Product Designers, 3rd edition*
  Tim Williams, Newnes, 2001 ISBN 0-7506-4930-5
- *EMC for Systems and Installations*
  Tim Williams and Keith Armstrong, Newnes 2000, ISBN 0-7506-4167-3
- *EMC for Systems and Installations*
  Keith Armstrong, EMC Compliance Journal, 1999, www.compliance-club.com/KeithArmstrongPortfolio
- *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

Some references for safety-related software

- *EMC and Electrical Safety Design Manuals,* York EMC Services, 2002, sales@yorkemc.co.uk, phone: +44 (0)1904 434 440
  - Volume 1 - What is EMC? ISBN 1-902009-05-3
  - Volume 2 - EMC Design Techniques - Part 1 ISBN 1-902009-06-1
  - Volume 3 - EMC Design Techniques - Part 2 ISBN 1-902009-07-X
  - Volume 4 - Safety of Electrical Equipment ISBN 1-902009-08-8
- IEC 61805-3: *Functional safety of electrical, electronic and programmable electronic safety-related systems – Software Requirements*
- *Noise, EMC and Real-Time*, MISRA Report 3, February 95. The Motor Industries Software Reliability Association (MISRA), http://www.misra.org.uk
- *Electromagnetic Compatibility of Software*, IEE Colloquium, Thursday 12th November 98, IEE Colloquium Digest: 98/471, sales@iee.org.uk

Emc4fs-2.5B CCC

Some references for safety-related software
continued...

- ***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 three references below are valuable for improving software immunity to all transients

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