Another EMC resource
from EMC Standards

EMC in Safety Cases

Helping you solve your EMC problems

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

EMC in Safety Cases

Why EMC testing is never enough

—

'Defence and Avionics' session, EMC-UK 2007

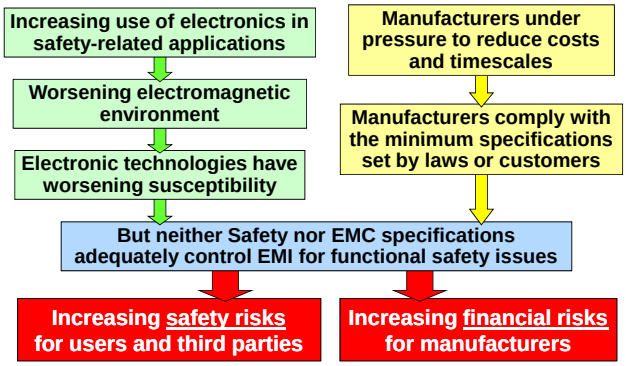
Cherry Clough Consultants
www.cherryclough.com

Eur Ing Keith Armstrong CEng MIET MIEEE ACGI
phone & fax: +44 (0)1785 660 247
keith.armstrong@cherryclough.com

Introduction to the problem

- Electronic technologies (including software) are being increasingly used in safety-related applications
- But modern technologies are increasingly likely to cause electromagnetic interference (EMI)…
  - ➔and are also increasingly susceptible to EMI…
  - ➔due to die shrinks; faster processing speeds; lower operating voltages; increased complexity of hardware and software; etc.

The result — EMI is increasing risks



Good safety engineering practices

- Equipment must be safe for its whole lifecycle…
  - ➔so safety cases are based upon the use of good engineering *design* principles for all safety issues, including software…
  - ➔using an approach based upon hazard assessment and risk analysis, that takes into account…
    - ◆the real-life environment and the effects of physical stresses and ageing…
    - ◆foreseeable faults, and foreseeable use/misuse
  - ➔see DEF STAN 59-411 Part 1, Annex H

But most safety cases treat EMI issues quite differently

- They assume that if new items of equipment pass conventional EM immunity tests, the systems they create will be safe enough (as far as EMI is concerned)…
  - ➔but EM testing ***cannot*** provide sufficient confidence that lifecycle safety is adequate (see later)…
  - ➔*just as for software*, the amount of testing required would be so large that no-one could possibly afford the time or the cost…
    - ◆EMC for functional safety actually requires a lifecycle *design-based* approach

Conventional immunity testing ignores foreseeable faults

- Safety must be maintained with (at least) one fault, but conventional EM testing ignores this, e.g…
  - ➔dry joints, open or short circuits
  - ➔out-of-tolerance or incorrect components
  - ➔missing or damaged conductive gaskets
  - ➔loose enclosure or cable shielding fixings
  - ➔failure of a surge protection device

Conventional immunity testing ignores foreseeable use/misuse

- Safety must be maintained despite foreseeable use or misuse, e.g…
  - ➔not following the correct operational procedures…
  - ➔operating with doors open or covers removed…
  - ➔mistakes, pranks, and malicious behaviour
- But conventional EM testing ignores these issues

Conventional immunity tests do not simulate real-life EM exposure

- Anechoic chambers are generally used for radiated RF tests…
  - ➔but they are unlike most real-life environments
- Reverberation (mode-tuned) chambers can provide much more realistic tests

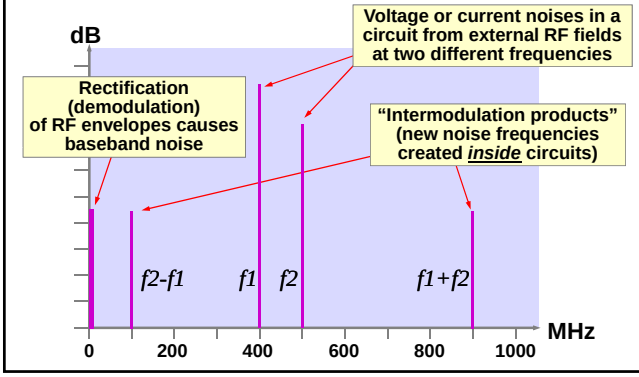
Conventional immunity tests do not simulate real-life EM exposure continued…

- RF susceptibility depends *strongly* on the modulation type and frequency…
  - ◆a fact that is used by electronic jamming specialists
- But for ease of testing and reproducibility conventional RF immunity testing uses a 1kHz square-wave (or sine-wave) modulation…
  - ➔so could prove *almost nothing* about the susceptibility to the <u>real-life</u> RF environment

Conventional immunity tests do not simulate real-life EM exposure continued…

- In real life, systems are often exposed to two or more simultaneous EM disturbances, e.g…
  - ➔two RF fields with different frequencies…
  - ➔an RF field plus a fast transient or ESD event
- Simultaneous RF fields with different frequencies can cause EMI through intermodulation…
  - ➔occurs in all non-linear devices (e.g. semiconductors)

Example of RF noises in a circuit showing demodulation and intermodulation



An example of intermodulation

- Conventional (single frequency) testing 10kHz - 18GHz discovers susceptibility over 50 - 500MHz…
  - ➔shielding and filtering that is effective over 50 - 500MHz added, equipment now passes the test
- But no protection added from (say) 5.0 - 5.5GHz…
  - ➔allowing simultaneous frequencies in this range to enter equipment and be intermodulated in devices
  - ➔creating ***<u>internal</u>*** noise over the range 50 - 500MHz, and causing interference

Conventional immunity tests do not simulate real-life EM exposure
continued…

- Conventional immunity tests apply one ***type*** of disturbance at a time…
  - ➔but in real life, transient events such as ESD or fast transient bursts (e.g. from opening electromechanical contacts) often occur at the same time as continuous RF fields…
  - ➔tests have shown that equipment that passes individual immunity tests can be very susceptible to *simultaneous* disturbances of different types

Conventional EM testing ignores the effects of the physical environment

- Mounting stresses (e.g. bending and twisting), shock, vibration, temperature extremes, exposure to liquids or conductive dusts…
  - ➔can all cause degraded EM performance, e.g. by reducing attenuation of shielding and/or filtering
  - ➔as can ageing, due to temperature cycling, humidity, corrosion, operational wear and tear, cleaning, etc.
  - ➔MIL-STD-464 includes annexes describing several examples of such real-life problems

Conventional EM testing ignores the effects of the physical environment
continued…

- For example: filters can be badly affected by higher than nominal ambient temperatures, supply voltages, and load currents…
  - ➔up to 20dB filter degradation has been measured due to combinations of temperature and load conditions…
    - ◆within the manufacturer's continuous ratings…
  - ➔when compared with the results achieved on the standard EM immunity tests

Conventional EM testing ignores the effects of the physical environment
continued…

- Equipment is often subjected to highly-accelerated lifecycle testing (HALT)…
  - ➔but the resulting 'aged' unit is generally not retested for its EM susceptibility

Conventional EMC standards ignore the quality of the EM design

- But if equipment was not *designed* to achieve a given level of EM immunity…
  - ➔despite component tolerances, semiconductor die-shrinks, variations in assembly, replacement of obsolete components, software bug fixes, etc…
  - ➔then the fact that an example unit once passed its EMC tests *means nothing at all* for the EM performance of the units actually supplied…
    - ◆if they were to be tested in the same way

Conventional EM testing ignores assembly errors

- Good safety engineering always requires some testing of each unit manufactured to make sure that assembly errors have not made it unsafe…
  - ➔but no conventional EMC test standards include routine checks for serial manufacture
- So we have no way of knowing if items of equipment actually supplied to users have significant EMI defects

Conventional EM testing ignores systematic effects

- It is often assumed that if all the items of equipment in a system pass their immunity tests…
  - ➔then systems constructed from them will have low levels of susceptibility
- But, due to 'emergent complexity' phenomenon…
  - ➔performance degradations that are acceptable for an item of equipment on its own (or are not measured during testing) could have significant implications for some systems

The maximum test level is not necessarily the worst

- All electronic devices are non-linear, and their circuits/software can be very complex…
  - ➔so they can sometimes fail when tested at low test levels…
  - ➔but fail in a different way (or even pass!) when tested at the maximum specified level…
  - ➔but most conventional EM tests only test at the highest test levels considered likely to occur in the environment

Conventional EM testing and COTS equipment

- The EMC test standards used by COTS equipment for their compliance (e.g. to the EMC Directive)…
  - ➔were developed using cost/risk trade-offs that took no safety applications into account
- So their test methods, procedures, and acceptable performance criteria might not be appropriate for their use in safety systems…
  - ◆it is not simply an issue of comparing the commercial test levels with those in the military/aerospace standards

We can't *afford* to rely solely on EM testing, where safety is concerned

- Achieving sufficient confidence in adequate levels of safety, using EM testing alone…
  - ➔would require a test programme no-one could afford
- So we need to be cleverer, to be able to demonstrate in our safety cases…
  - ➔that the EM performance will *reliably* ensure the required levels of safety risks…
  - ➔over the anticipated lifecycle

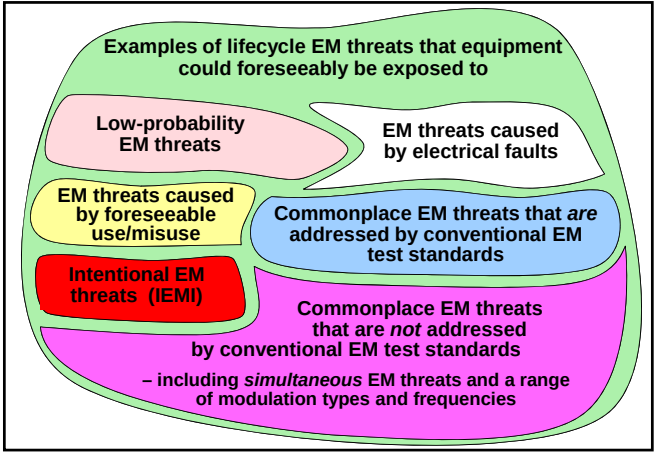
The cleverness required is achieved by: *appropriate EM Design*

- The EM design must ensure the necessary EM performance over the anticipated lifecycle
  - ➔taking the reasonably foreseeable EM and physical environments into account
- Safety cases must document the EM design…
  - ➔plus how it was validated and verified to achieve the required confidence…
    - ◆using a range of techniques, usually including some (affordable) EM testing

Safety Cases should include…

(see clause H.7 in DEF STAN 59-411 Part 1, Issue 1)

- An assessment of the real-life EM environment(s) over the anticipated lifecycle…
  - ➔usually requires much more work than simply copying the data from the test standards…
    - ◆e.g. assessment of modulation types/frequencies, simultaneous disturbances, foreseeable misuse, future changes to the environment, etc.
- An assessment of the real-life physical environment(s) over the anticipated lifecycle…
  - ◆mechanical, climatic, biological, wear-and-tear, etc.



Safety Cases should include… continued…

- An assessment of how the design could *possibly* be affected by its lifecycle EM and physical environment(s)…
  - ➔taking into account faults, misuse, etc…
- A hazard analysis and risk assessment that takes the above fully into account…
  - ➔and documents how any excessive safety risks were reduced to an acceptable degree by design changes

Safety Cases should include… continued...

- An overall Safety Requirement Specification (SRS) for the final safety system…
  - ➔that includes the EM and Physical requirements specifications resulting from the above
- Equipment Requirement Specifications (ERSs) for each item of equipment used in the system…
  - ➔taking any EM or physical mitigation measures applied in the system into account…
    - ◆showing how these were derived from the SRS

Safety Cases should include… continued...

- A verification / validation plan providing sufficient confidence in the EM and physical design…
  - ◆and also in the implementation / realisation /assembly / construction
  - ➔employing a mixture of activities, such as predictions, reviews or tests, e.g…
    - ◆Verified computer simulations
      Demonstrations
      Inspections
      Independent assessments
      Some EM tests on items of equipment, and on the completed safety system
      Checklists
      Reviews and audits

Although testing can never be sufficient, it is a very powerful verification technique

- EM / physical testing should replicate the real-world environment(s) as closely as possible…
  - ➔based on standardised test methods and procedures, expertly modified as appropriate
- A number of experts already do this

Safety Cases should include… continued...

- The results achieved by the verification / validation activities…
  - ➔and details showing how any shortcomings were dealt with so as to achieve the SRS for the safety system
- Any measures necessary to maintain safety over the lifecycle….
  - ➔e.g. checking any assumptions that were originally made about real-life EM and physical environments

The amount of work required

- Where higher levels of 'safety integrity' (e.g. SILs under IEC 61508) are required…
  - ➔more detailed and comprehensive work will be required…
  - ➔in the assessment of the environments, specifications, design…
  - ➔and in their validation and verification

Conclusions

- EM testing is inadequate when used as the sole method of ensuring EM performance for safety…
  - ➔lifecycle EM engineering methods like those already used for *all other safety* issues (including software) are required….
  - ➔including appropriate EM design and verification techniques…
  - ➔and should be documented in the Safety Case

EMC in Safety Cases

Why EMC testing is never enough

—

'Defence and Avionics' session, EMC-UK 2007

the end

Cherry Clough Consultants

www.cherryclough.com

Eur Ing Keith Armstrong CEng MIET MIEEE ACGI
phone & fax: +44 (0)1785 660 247
keith.armstrong@cherryclough.com

Some useful references

- Keith Armstrong, *New Guidance on EMC-Related Functional Safety,* 2001 IEEE EMC International Symposium, August 13-17 2001, ISBN 0-7803-6569-0, pp. 774-779
- Keith Armstrong, *New Guidance on EMC and Safety for Machinery,* 2002 IEEE International EMC Symposium, Minneapolis, August 19 - 23, ISBN: 0-7803-7264-6, pp. 680-685
- Keith Armstrong, *Review of Progress with EMC-Related Functional Safety*, 2003 IEEE EMC Symposium, Boston, August 18-22 2003, ISBN 0-7803-7835-0 pp 454-459
- Keith Armstrong, *Why EMC Immunity Testing is Inadequate for Functional Safety*, 2004 IEEE International EMC Symposium, Santa Clara, USA, August 9-13 2004,ISBN 0-7803-8443-1, pp 145-149 — also Conformity, March 2005 pp 15-23, http://www.conformity.com

Some useful references continued…

- Keith Armstrong, *Functional Safety Requires Much More Than EMC Testing*, EMC-Europe 2004 (6th International Symposium on EMC), Eindhoven, The Netherlands, September 6-10 2004, ISBN: 90-6144-990-1, pp 348-353
- Keith Armstrong, *Introduction to EMC for Functional Safety,* EMC-UK 2004, Newbury, UK, 12-13 October 2004, pp 116-123 — also in the EMC Society of Australia Newsletter, June 2005, Issue No. 30, pp 8-16, http://www.emcsa.org.au
- Keith Armstrong, *Specifying Lifecycle Electromagnetic and Physical Environments – to Help Design and Test for EMC for Functional Safety,* 2005 IEEE International EMC Symposium, Chicago, USA, August 8-12 2005, ISBN: 0-7803-9380-5, pp 495-499

Some useful references continued…

- Keith Armstrong, *Design and Mitigation Techniques for EMC for Functional Safety*, 2006 IEEE International Symposium on EMC, 14-18 August 2006, Portland Oregon, ISBN: 1-4244-0294-8
- Keith Armstrong, *Validation, Verification and Immunity Testing Techniques for EMC for Functional Safety*, 2007 IEEE International Symposium on EMC, 9-13 July 2007, Honolulu, Hawaii, ISBN: 1-4244-1350-8
- Guidance document on EMC and Functional Safety, The IET (London, UK) 2000, http://www.theiet.org/publicaffairs/sectorpanels/emc/index.cfm
- List of resources on EMC and Functional Safety, compiled by Keith Armstrong, http://www.iee.org/OnComms/PN/emc/EMCandFunctionalSafety.cfm

Some useful references continued…

- IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems* (seven parts)
- IEC 61508-3 *Functional Safety of Electronic/Electronic/Programmable Electronic Safety-Related Systems – Part 3: Software Requirements*
- 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*
- MIL-STD-464, Department of Defense Interface Standard – *Electromagnetic Environmental Effects – Requirements for Systems*. Typing "MIL STD 464" into the Google search engine finds free download sites. There are several other US Military standards that have useful requirements or guidelines on EMC design, including MIL-HDBK-1857, MIL-HDBK-419 and MIL-STD-1310G

Some useful references continued…

- Michel Mardiguian, *Combined Effects of Several, Simultaneous, EMI Couplings,* 2000 IEEE International Symposium on EMC, Washington D.C., August 21-25 2000, ISBN 0-7803-5680-2, pp. 181-184
- Jansson, L., and M. Bäckström, *Directivity of Equipment and its Effect on Testing in Mode-Stirred and Anechoic Chamber*, IEEE Int. Symposium on EMC, Seattle, WA, August 1999
- Freyer, G. J., *Distribution of Responses for Limited Aspect Angle EME Tests of Equipment with Structured Directional Directivity*, The 2003 Reverberation Chamber, Anechoic Chamber and OATS Users Meeting, Austin, TX, April 2003
- Freyer, G.J., and Hatfield, M.O., *An Introduction to Reverberation Chambers for Radiated Emission/Immunity Testing*, ITEM 1998, The International Journal of EMC, 1998

Some useful references continued…

- Freyer, G.J., Considerations for EMC Testing of Systems with Safety and/or Reliability Requirements, EMC Europe 2004, Eindhoven, The Netherlands, September 6-10 2004
- F Beck and J Sroka, *EMC Performance of Drive Application Under Real Load Condition*, Schaffner EMV AG application note, 11th March 1999
- W H Parker, W Tustin and T Masone, *The Case for Combining EMC and Environmental Testing*, ITEM 2002, www.rbitem.com, pp 54-60
- William A Radasky, "*2007 Update on Intentional Electromagnetic Interference (IEMI) and High Altitude Electromagnetic Pulse (HEMP)*", Interference Technology's 2007 EMC Directory and Design Guide, pp 143-148, www.interferencetechnology.com