Another EMC resource
from EMC Standards

Functional Safety requires much more than EMC testing

Helping you solve your EMC problems

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

Functional Safety requires much more than EMC testing

Cherry Clough Consultants

www.cherryclough.com

EurIng Keith Armstrong C.Eng MIEE MIEEE ACGI
Phone & Fax: +44 (0)1785 660 247
Email: keith.armstrong@cherryclough.com

NorthWest Compliance Association, 11th May 2005

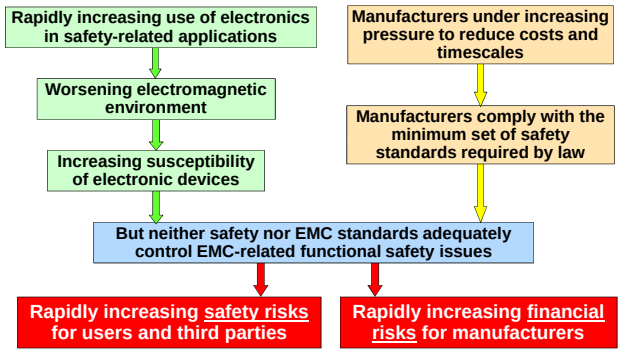
But its not just Functional Safety

- This presentation addresses the issue of EMC for Functional Safety
- But the same issues are equally important for equipment that…
  - ➔must have high-reliability (e.g. Internet and telecomms infrastructure)
  - ➔is mission-critical
  - ➔is involved in legal metrology (e.g. covered by the Measuring Instruments Directive)
  - ➔or where errors or failures can be costly

Functional Safety requires much more than EMC testing

- Electronics increasingly used in safety-related applications
  - ➔but modern technologies are more likely to cause interference
  - ➔*and* are increasingly vulnerable to interference
    - ◆ due to die shrinks, faster speeds, lower operating voltages, etc.
- But most safety standards don't cover interference and conventional EMC standards don't cover safety
  - ➔and most manufacturers only do the minimum permitted by EMC and safety standards
- *RESULT?* – risks due to interference are rapidly increasing

Increasing functional safety risks related to EM performance



EMC requirements in safety standards

- EMC requirements are being added to some safety standards
  - ➔IEC/TS 61000-1-2 aims to become the basic IEC standard that covers this issue
    - ◆it employs the hazards/risks approach recommended by the IEE's guide (www.iee.org/Policy/Areas/Emc/index.cfm) and (to some extent) by MIL-STD-464
  - ➔but most/all other safety standards so far rely solely on conventional immunity testing methods instead
    - ◆similar to testing for compliance with the EMC Directive (although usually with slightly higher test levels)
  - ➔although this approach is *totally inadequate* for safety

Comparison of traditional approaches taken by EMC immunity, and safety standards

- EMC immunity testing is always done on new equipment
  - ◆with no investigation of its design, or any consideration of lifecycle effects on EMC performance
- But equipment must be safe for its *whole lifecycle*…
  - ➔which is why safety standards have always specified good *safety design principles* for all other safety issues, *including software*, taking into account…
    - ◆foreseeable faults, use and misuse
    - ◆effects of lifecycle physical stresses and ageing
  - ➔so EMC for functional safety requires a '*lifecycle*' design-based approach — unlike conventional EMC compliance

Conventional immunity testing only covers one EM disturbance at a time

- In real life, equipment is subjected to multiple simultaneous EM disturbances
  - ➔of the same type, and of different types
  - ➔but conventional immunity tests apply one disturbance at a time
- Michel Mardiguian has shown that when one EM disturbance is applied (e.g. a radiated RF field) [7]
  - ➔the immunity of the equipment to another disturbance (e.g. fast transient bursts, ESD, etc.) can be seriously compromised

Conventional immunity tests do not simulate real-life EM exposure

- Anechoic chambers are unlike most real-life environments
  - ◆reverberation chambers can be used to get more realistic results
- The waveforms used for transient/surge/ESD tests might not correlate well with exposure to real-life disturbances
- The frequency of modulation of an RF threat can be critical to the immunity of an equipment
  - ◆this is well-known to electronic warfare experts
  - ➔but conventional RF immunity testing only uses a 1kHz sine-wave modulation (plus 0.5Hz for some medical equipment)

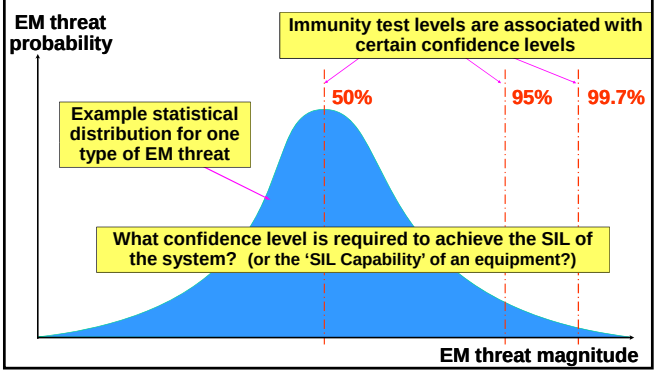
EMC 'risk analysis' is not normally done

- "EMC Directive" immunity tests are ***supposed*** to simulate the 'normal' EM environment...
  - ➔but they ignore the close proximity of mobile radio transmitters even though they are now a normal part of the EM environment
    - ◆e.g. walkie-talkies, cellphones, Bluetooth, Wi-Fi, etc.
  - ➔and they ignore almost all EM disturbances at less than 150kHz, and at more than 1GHz
    - ◆e.g. due to traction currents; cellphones at 1.8 - 2GHz, wireless datacomm's and ISM equipment at 2.45 and 5GHz, radar, etc.
  - ➔and they ignore the ±6kV (approx.) overvoltages known to occur annually on normal low-voltage AC supplies in Europe, USA
    - ◆due to thunderstorms and reactive load-switching

Conventional immunity testing "Compatibility Levels" may be too relaxed

- All EM disturbances vary statistically
  - ➔and conventional immunity standards typically assume 'compatibility levels' that cover 95% of their occurrences
    - ◆the 2-sigma level
  - ➔e.g. when RF immunity testing at 3 or 10V/m
- But 95% might be nowhere near good enough for some safety-related applications
  - ➔which might need to have confidence that they will be unaffected by more than 99.9% of EM disturbances (for example)

Conventional immunity testing "Compatibility Levels" may be too relaxed continued...



Foreseeable faults are not addressed by conventional immunity testing

- Equipment must remain safe despite one fault (at least)
- But conventional immunity testing does not consider the possibility of faults, for example…
  - ➔dry joints or short circuits (possibly ruining filter performance)
  - ➔out-of-tolerance or incorrect components, or unwitting use of a 'die-shrunk' integrated circuit
  - ➔conductive gaskets missing or damaged during assembly, or loose fixings in enclosure or cable shielding assemblies
    - ◆possibly ruining shielding performance
  - ➔failure of a surge protection device

The effects of the physical environment on EM performance are not considered

- Filters can be badly affected by higher than nominal ambient temperatures, supply voltages, and load currents
  - ➔because they can affect the parameters of the filters' inductors
    - ◆up to 20dB overall filter degradation has been measured
- Mounting stresses, shock, vibration, temperature extremes, exposure to liquids, conductive dusts, can all cause degraded EM performance
  - ➔as can ageing due to temperature cycling, humidity, corrosion, wear and tear, etc.
- But conventional EMC testing ignores these vital issues

Only a representative sample is usually tested for EMC

- If an equipment isn't designed to guarantee an appropriate level of EM performance in batch or volume manufacture…
  - ➔despite variations in components and assembly, replacement of obsolete components, bug fixes, design improvements, etc.,
- The EM performance of supposedly identical products can vary significantly
  - ➔the fact that one of them passed its EMC tests means *nothing*
- This issue is ignored by conventional immunity testing
    - ◆which typically only tests one example of a new design, tested in a benign physical environment

Conventional EMC testing ignores maintenance, repair, refurbishment, upgrades, etc.

- Real equipment is subject to cleaning and maintenance
  - ➔during which shielding doors and covers may be opened (for e.g.)
- It is also subjected to repair, refurbishment, modifications and upgrades
- Most safety test standards take some/all of these issues into account
  - ➔as a matter of good safety engineering practice
  - ➔but conventional EMC testing standards do not

Performance degradations acceptable for EMC might not be acceptable for safety

- Systems are generally only tested for EMC at the level of their individual items of equipment
  - ➔but performance degradations that are acceptable for an equipment on its own could increase systematic safety risks
- E.g. a 24V dc power supply might meet 'Performance Criterion B' on a fast transient burst test
  - ➔by switching its output off for a short time
  - ➔but this might be unacceptable for the safety functions controlled by microprocessors powered from the 24V dc supply

How EMC *should* be controlled for functional safety

- The IEE's Guide recommends using a hazards and risk assessment approach as follows:

A) What EM threats could the equipment foreseeably be exposed to?

B) What could foreseeably happen as a result of the EM threats identified by A) above?

C) Could the foreseeable EM emissions from the equipment affect other equipment?

How EMC should be controlled for functional safety continued...

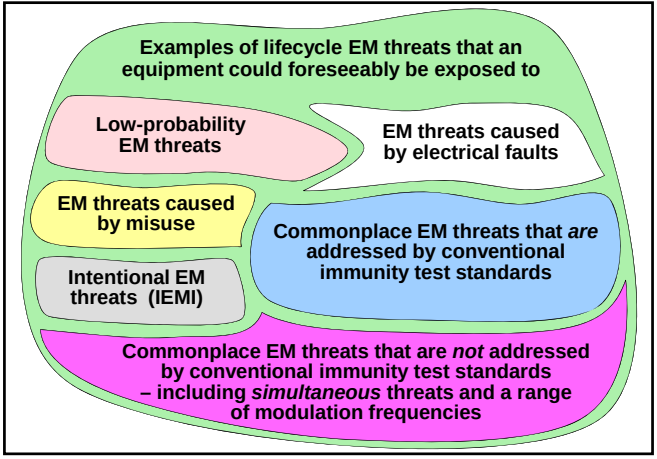
D) What are the foreseeable implications of A) - C) above for functional safety?

E) What actions are needed to achieve the required level of functional safety?
e.g. design and verification; QA

F) What documentation is required to show that due diligence has been applied?

A) What EM threats could the equipment foreseeably be exposed to?

- EM 'threats' are more correctly called: EM disturbances, or EM phenomena
  - ➔and EM interference (EMI) is what happens when the equipment is not compatible with its EM environment
- An 'EM threat assessment' is required
  - ➔for the foreseeable EM environment of the equipment's intended operational site(s)
  - ➔taking into account low-probability EM threats over its lifecycle
    - ◆a guide to assessing an EM environment can be downloaded from www.cherryclough.com



Modified trams in Helsinki interfered with equipment in a hospital along their route

B) What could (foreseeably) happen ?

- *Electromechanical* devices can malfunction, and be damaged
  - ➔especially a problem for 'hard-wired' safety systems
- *Analogue circuits* can be upset, and damaged
  - ➔especially a cause of errors in instrumentation
- *Digital circuits* and programmable devices can malfunction, and be damaged
  - ➔especially a problem for control and automation

Erection of the Millennium Wheel (London Eye) was delayed by interference from outside broadcast vehicles' satellite dishes

C) Foreseeable effects of equipment emissions

- Emissions standards are *not* intended to protect nearby radio receivers or other sensitive circuits
  - ➔and some permit very high levels in specified circumstances, enough to...
    - ◆be a direct hazard to human health
    - ◆cause serious interference with electronic devices
- So the foreseeable effects on existing equipment of the *emissions* from the new equipment...
  - ➔should be considered in the hazards assessment and risk analysis

D) What are the reasonably foreseeable functional safety implications?

- This should take into account:
  - ➔the severity of the possible safety hazard
  - ➔and the scale of the risk
- It is best to employ the approach of IEC 61508
- Remember that exposure to EM threats, and the equipment's responses to the threats, both have statistical probabilities
  - ➔a bit like predicting the "100-year" gale or wave

Some early ABS systems were interfered with by powerful CB radios in trucks

E) What actions are needed to achieve the required level of safety?

- Five kinds of actions are needed
  - ➔carried out in the following order...

E1) Hazard reduction by design

- Design so that the safety functions have less demanding requirements
  - ➔for the equipment's whole lifecycle

What actions are needed? continued...

E2) EMC risk-reduction by design

- The EMC performance of the protection measures should be designed to be reliable over the equipment's whole lifecycle

E3) Verification of the design techniques employed

- Testing that simulates the foreseeable EM environment, plus the foreseeable physical environment, faults, misuse, etc., over the equipment's whole lifecycle

What actions are needed? continued...

E4) Maintenance of safety performance in serial manufacture, maintenance, repair

- EMC performance can be made worse by...
  - ➔a different batch of ICs
  - ➔the surface conductivity of metalwork and its fixings
  - ➔an altered cable routing
  - ➔other small changes in assembly
  - ➔'form, fit and function' replacement parts
  - ➔changed suppliers for parts, and processes (e.g. painting)

What actions are needed? continued...

- So a Quality Assurance (QA) system is required that controls all of the safety aspects of the equipment during manufacture (including EMC)
- This QA system should control…
  - ➔components, sub-assemblies, software (whether bought-in, or made-in-house)
  - ➔in-house processes (e.g. plating) and subcontractors
  - ➔manufacturing concessions, design changes
  - ➔the final build standard of the equipment

What actions are needed? continued...

E5) Maintenance of safety performance despite modifications and upgrades

- ➔a QA system is required that controls all of the safety aspects of the equipment, including EMC-related safety for the above activities
  - ◆it will be very similar to the procedure used to ensure that EMC-related safety aspects were correctly addressed during the equipment's original design

Safety design, verification and QA activities over the "equipment's lifecycle" should take into account...

- ➔Design and development
- ➔Manufacture
- ➔Storage
- ➔Transport
- ➔Installation
- ➔Commissioning
- ➔Operation
- ➔Maintenance
- ➔Repair
- ➔Refurbishment
- ➔Decommissioning
- ➔Disposal

The steering of an Australian Navy minesweeper was affected by the radar of a nearby ship, nearly causing a collision

F) What documentation is required to show due diligence?

- If it isn't written down... the law assumes it didn't happen
- So the project records should show that steps A) to E) above were carried out in full
  - ➔that the required EMC performance was determined and 'designed-in'
    - ◆for all safety-related areas, from the start of a project
    - ◆and verified at the end of a project

This has only been an introduction

- These issues, and the necessary actions are discussed in much more practical detail in our training courses on EMC for Functional Safety
  - ➔available as half-day, one-day and two-day courses
  - ➔and also in the IEE's one-day courses, which I teach in partnership with Simon Brown of the HSE

Conclusions

- Functional Safety requires a ***lifecycle*** approach to EMC
  - ➔immunity testing has an important part to play in the achievement of functional safety
  - ➔but conventional immunity test methods are *clearly inadequate* for this purpose
- EMC lifecycle safety engineering methods similar to those already used for <u>all other safety issues</u> (including software) should be employed
  - ➔**appropriate EMC *design* and *verification* techniques, and *QA*, are required over the lifecycle**

Functional Safety requires much more than EMC testing

the end

Cherry Clough Consultants

www.cherryclough.com

Eurlng Keith Armstrong C.Eng MIEE MIEEE ACGI
Phone & Fax: +44 (0)1785 660 247
Email: keith.armstrong@cherryclough.com

Some useful references

- *Guide on EMC & Functional Safety*, The IEE (London, UK) 2000, http://www.iee.org/Policy/Areas/Emc.index.cfm
- *Assessing an EM Environment*
  useful tables, procedures, sources, and simple calculations
  download via http://www.cherryclough.com
- The EMC & Compliance Journal 2004 'Yearbook' CD-ROM with a wealth of useful information including the following…
  - ➔Designing for EMC (6 parts)
  - ➔EMC for Systems and Installations (6 parts)
  - ➔EMC Testing (7 parts) (from low-cost D-I-Y to full compliance)
  - ➔The "Banana Skins" Compendium (EMI anecdotes)
  - ➔available from http://www.compliance-club.com

Some useful references continued...

- *EMC for Functional Safety*, IEE (London, UK) training course (first held February 10th 2004), http://www.iee.org.uk, contact: amani@iee.org.uk
- *List of Resources on EMC and Functional Safety*, http://www.iee.org/OnComms/PN/emc/EMCandFunctionalSafety.cfm
- 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*
- *Functional Safety and EMC*
  Simon J Brown and Bill Radasky, presented at the IEC Advisory Committee on Safety (ACOS) Workshop VII, Frankfurt am Main, Germany, March 9-10 2004

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*
- *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
- *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

Some useful references continued...

- *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
- *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 magazine, March 2005 pp 15-23, download via http://www.conformity.com.
- *Functional safety requires much more than EMC testing*
  Keith Armstrong, EMC-Europe 2004 (6th International Symposium on EMC), Eindhoven, The Netherlands,
  September 6-10 2004, ISBN: 90-6144-990-1, pp 348-353

Some useful references continued...

- *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 and J Sroka, Schaffner EMV AG application note, 11th March 1999
- *The Case for Combining EMC and Environmental Testing*
  W H Parker, W Tustin and T Masone, ITEM 2002, pp 54-60, http://www.rbitem.com