Another EMC resource
from EMC Standards

EMC for Functional Safety - The Need for Independent Assessment

Helping you solve your EMC problems

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

Keith Armstrong

EMC for Functional Safety — The Need for Independent Assessment

Cherry Clough Consultants

www.cherryclough.com

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

Meeting of IET/BCS ISA working group, Savoy Place, London, May 12, 2008

FSemc15a CCC

Introduction to EMC for Functional Safety

- Safety-related systems must maintain adequately low risks over their entire lifetimes
- Where electromagnetic interference (EMI) could affect risks…
  - an adequate level of electromagnetic (EM) performance is required over the system's lifetime…
  - this is known as… '*Electromagnetic Compatibility for Functional Safety*'
    - or simply: '**EMC for Functional Safety**'

FSemc15a CCC

Introduction continued…

- ***EMC for Functional Safety*** is becoming more important as more safety functions are relying on the correct operation of electronic technologies…
  - especially those running software/firmware
- But the existing approach to EMC is totally inadequate for safety engineering…
  - so a new approach is needed…
    - just as a new approach was required to be able to use, verify & validate software for safety related applications

FSemc15a CCC

Introduction continued…

- Actual EM performance is affected by the physical environment, e.g….
  - mechanical forces; shock and vibration; temperature; humidity; exposure to liquids, gasses, dusts, vapours; air pressure; mould growth, etc.
  - ageing, including corrosion, fretting, wear, etc.
  - foreseeable use and misuse
  - faults in components, wiring, enclosures, etc.

FSemc15a CCC

Introduction continued…

- Real-life EM and physical environments can be very complex…
  - they do not *always* consist of single EM or physical disturbances applied one-at-a-time…
  - tests have shown that EM performance can suffer very significantly when multiple EM disturbances, and/or EM + physical disturbances, are applied simultaneously
- The EM performance of a system *cannot* be predicted solely from the EM characteristics of its component parts (an example of 'emergent behaviour')

FSemc15a CCC

Introduction continued…

- Result: ***It is not practical to prove that systems are safe enough solely by EMC testing !***
  - ***no-one*** could afford the necessary test plan
- So: cost-effectively ensuring acceptable safety risks requires the ***application of appropriate EM/physical design techniques***…
  - based on the reasonably foreseeable worst-case EM and physical environments over the anticipated lifetime, use/misuse, faults, etc.

Keith Armstrong

FSemc15a CCC

The need for design assessment

- The EM/physical design techniques employed should be verified & validated by competent people
- Some EM and physical testing will be required, but these will generally not be standard EMC tests…
  - they will usually be tailored to the design, environment and the application (and SIL)…
  - so their planning and results will also need competent assessment

FSemc15a CCC

The need for design assessment continued…

- The following slides briefly mention some of the appropriate verification & validation techniques that will require competent assessment
- The higher the SIL: the greater the requirements for…
  - Expertise of the assessors
  - Depth of assessment (including amount of work)
  - Independence of the assessors

FSemc15a CCC

Appropriate verification & validation methods for EMC design include…

- *Demonstrations*
  - e.g. demonstrating that the functional safety requirements have been correctly implemented
- *Checklists*
  - e.g. to ensure that the necessary EMC design measures have been applied

FSemc15a CCC

Verification & validation methods include… continued…

- *Inspections*
  - e.g. checking that the assembly and installation have followed the designers' EMC requirements correctly
- *Design Reviews*
  - ensure compliance with the objectives of each phase of the project lifecycle

FSemc15a CCC

Verification & validation methods include… continued…

- *Individual or integrated hardware tests*
  - different parts of the system are assembled step-by-step, with checks/tests that ensure confidence at each step
- *Validated computer modeling*
  - ◆ now routinely used in some critical industries to reduce design/test times/costs without sacrificing reliability
  - once a model is well-enough proven by comparison with appropriate EM tests, it can be used to quickly simulate numerous similar tests that would be too costly or time-consuming to perform in real-life

FSemc15a CCC

Verification & validation methods include… continued…

- *Audits*
  - e.g. checking that the correct processes have been followed in…
    - Specification
    - Design
    - Assembly
    - Installation
    - Validation/verification
  - audits are essentially quality assurance (QA) activities

Keith Armstrong

FSemc15a CCC

Verification & validation methods include… continued...

- *Non-standardized checks and tests*
  - people tend to think of EMC testing only in terms of the standardised laboratory test methods (e.g. MIL-STD-461, IEC 61000-4-x, etc.)
  - but there are many non-standard EM/physical checks and tests that can be used to improve confidence in the EM and physical design..
  - and hence in its achievement of acceptable safety risks as regards the possibility of EMI…
    - often designed specifically for a project

FSemc15a CCC

Verification & validation methods include… continued...

- *Formal EMC Testing*
  - that helps verify the EM/physical design
- An EMC test plan that could give sufficient design confidence will ***always*** be much too lengthy, and cost too much…
  - however, ***appropriately-designed EMC testing*** is a powerful verification/validation technique for safety-related equipment and systems

FSemc15a CCC

EMC Testing that helps verify the EM/physical design continued...

- Tests should be done on the highest practicable level of system integration (e.g. 'in-situ' or 'on-site')…
  - where these are impractical, tests should be carried out on individual items of equipment (system components)…
    - e.g. EM mitigation (shielding, filtering, etc.) can be assembled and tested *before* the system is complete
  - always taking care to realistically simulate the actual EM environment, and the complete system…
    - e.g. simultaneously exposing redundant channels to the same EM stresses

FSemc15a CCC

Foreseeable faults, use and misuse

- The design should have taken these into account…
  - so these design aspects will need to be verified to achieve sufficient confidence in the system's safety
  - e.g. by analysis, or by repeating other checks or tests whilst simulating the faults, use or misuse
  - careful planning should ensure that such tests add usefully to confidence, without disproportionate times and costs

FSemc15a CCC

Assessment is required from very early in a project

- Lengthy or costly design verification or validation requirements can sometimes be avoided by doing the design in a different way…
  - so for cost-effectiveness, verification & validation planning should be done during the 'definition' phase of a project (before the design phase starts)…
  - and may need to be modified as the design progresses

FSemc15a CCC

After installation, during use

- Design and its verification/validation were based on assessments of the worst-case EM and physical environments…
  - and on how they, and their mitigation measures, will probably change over time (e.g. wear, ageing)…
- So to control safety risks it can be necessary to verify such assumptions regularly during the lifetime…
  - and the planning and implementation of these activities will also need assessment

Keith Armstrong

FSemc15a CCC

The current availability of competent EMC assessors

- The 'EMC world' hardly understands functional safety engineering *at all*…
  - and the 'safety world' does not generally understand how real-world EMC can affect safety
- Most EMC experts are academics, or experts in applying standardised EMC tests…
  - although there are some good people involved in military and avionics
- So the required competency does not yet exist

FSemc15a CCC

EMC for Functional Safety — The Need for Independent Assessment

the end

Cherry Clough Consultants

www.cherryclough.com

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