emc STANDARDS

Another EMC resource
from EMC Standards

Functional Safety requires much more than EMI testing (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

Functional Safety requires much more than EMI testing

by Keith Armstrong

This is the second part of a two-part article, published in 'Safety Systems', the Safety-Critical Club Newsletter, Volume 17, Number 1, September 2007, pp 1-5

The first part of this article (published in Vol. 16, No. 3 of Safety Systems) showed why electromagnetic (EM) immunity testing cannot be relied upon, on its own, to demonstrate that a safety system that relies upon electronic devices and/or software will have low enough risks due to interference from its operational (real-life) electromagnetic environment(s). This second part discusses what should be done in addition.

1. Design techniques for EMC for functional safety

Special 'final equipment' EM immunity test methods can help contribute to confidence in functional safety performance. Examples of such methods include the EM immunity tests in RTCA/DO160E [1] and MIL-STD-461E [2]. But when the issues mentioned above are taken into account, it can be shown that even these excellent EMC test standards are unable, on their own, to demonstrate that safety risks due to electromagnetic interference (EMI) will remain low enough over the anticipated lifetime.

Proving that adequate safety has been achieved by using immunity testing alone would require a test programme that no one could afford. So we need to be cleverer, to achieve the required safety integrity with reasonable costs and timescales.

Just as for all other safety issues (including software, see Part 3 of [3]) appropriate EM design techniques are required, verified and validated by a number of methods (probably including appropriately designed EM and physical tests).

1.1 Assessing the lifecycle EM and physical environments

Designing the EM performance of a system so that it performs its safety functions with sufficient reliability over its lifecycle depends upon knowing the worst-case EM and physical environments it could be exposed to. So, a thorough assessment of the reasonably foreseeable lifecycle environments is a necessity, and Figure 1 indicates some of the relevant issues for the EM environment.

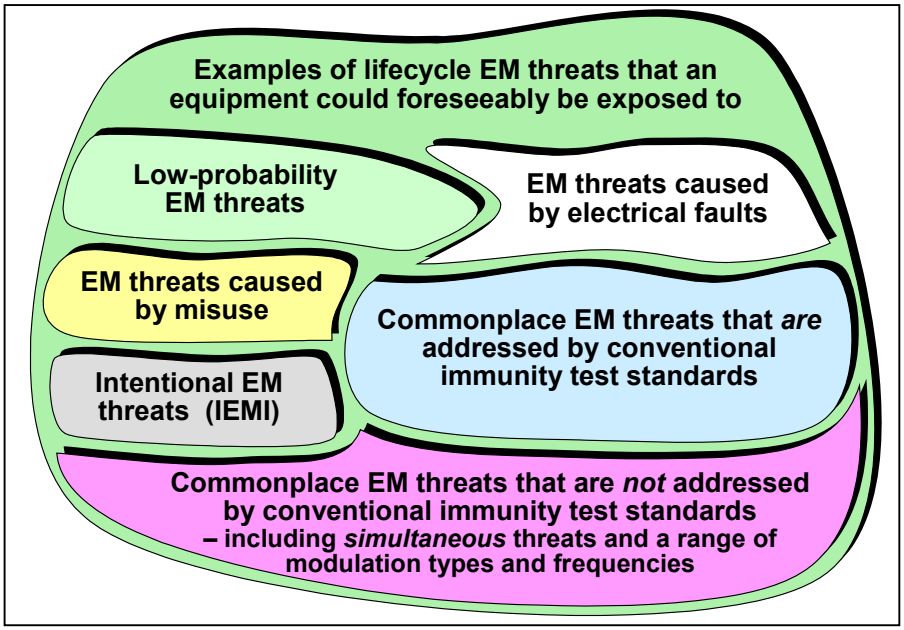

Figure 1: Assessing an EM environment

Because adequate safety must be achieved for an equipment's whole life, the EM design must take into account the reasonably foreseeable physical environment (mechanical, climatic, chemical,

biological, etc.) over the lifecycle, plus foreseeable faults, ageing, misuse, etc. [4] describes how to go about assessing worst-case EM and physical environments.

1.2 Determining the natural susceptibilities of a design

Testing an item of equipment with its EM mitigation removed reveals the frequencies at which it is naturally susceptible. Assessment of the EM environment (see 4.1) then reveals how those natural susceptibilities could be excited, taking into account direct interference; demodulation and intermodulation.

EM mitigation measures are then designed to protect the equipment from the possibilities revealed by the above analysis. This more 'targeted' approach to mitigation helps achieve higher levels of confidence with lower overall costs.

1.3 Fault misuse assessment and mitigation

Failure analysis and brainstorming discover what faults and misuse could compromise EM performance, and the design takes these into account.

1.4 EM design that copes with the lifecycle physical environment

For example:

- Shielding gaskets should be designed to have sufficient compression to cope with foreseeable movements in the gaps they fill, despite the physical stresses that could be applied. Materials should not suffer excessively from galvanic corrosion or other ageing effects due to the physical environment for the anticipated life. Gaskets should be designed to withstand foreseeable lifecycle wear-and-tear (e.g. at doors and panels that might be frequently opened).
- Filter grounding should use multiple electrical bonds, using anti-vibration fixings to reduce the likelihood of an open-circuit to acceptably low levels. Component over-rating and encapsulation can reduce possible damage from shock, vibration and many other environmental 'threats'.

1.5 Monitoring, and safe shut-down techniques

Protection circuits can often be used to detect malfunction and shut down safely, or force operation into a safe default mode. They can also be used to protect from malfunctions caused by EMI.

The EM environment can be monitored and safe shut down/default initiated if extreme EM events occur. This helps overcome the difficulty of determining the worst-case lifecycle EM environment. If such EM monitoring is located within a shielded enclosure, it also detects unexpected degradation of its EM performance, for example due to its misuse (e.g. operation with a door open) or the wear-out of some critical part. EM detectors responding from a few MHz to many GHz are commercially available.

1.6 'Multilayered' mitigation measures are more reliable

'Multilayering' techniques provide redundancy that can help protect against unforeseen situations. For example: an enclosure with a shielding effectiveness (SE) of 90dB at 900MHz can have its SE reduced to just 20dB by someone drilling a 15mm diameter hole in it (e.g. to add an indicator lamp).

However, if using three 'nested' shields each achieving 30dB (e.g. overall cabinet; chassis unit; printed circuit board) – even complete destruction of the outermost shield would still leave an SE of 60dB. (Also, the three 30dB shield layers could cost less than one 90dB enclosure.)

1.7 Redundant channels employing diverse technologies

IEC 61508 calls EMI a 'common-cause' phenomenon: malfunctions due to EMI are not random, and for a given design will always occur when certain conditions obtain. EMI failures are 'designed-in'.

One way to improve the reliability of electronics is to employ multiple redundant 'channels' with a 'voting' arrangement so that if one or more channels malfunction the preponderance of other channels providing the correct output will maintain correct operation. For this approach to improve fault tolerance for common-cause faults such as EMI, it is necessary to use 'diverse technologies' – each channel in the redundant array should be physically realised sufficiently differently that it will not react in the same way to the same EM events.

1.8 Using fibre-optics instead of conductors for signal or data

Fibre-optic cables carrying signals or data are perfectly immune to all EM phenomena, at all conceivable levels, over any period of time. Conducting interconnection systems generally cost less to purchase, but their overall cost of ownership can easily turn out to be much higher than fibre-optic systems.

1.9 Design reviews with independent experts

This helps avoid the problems caused by 'blind spots' in the corporate culture, and/or a lack of sufficient expertise in the personnel employed on the project.

2. Verification of the EM design

A wide variety of validation and verification techniques should be used. Suitable methods include…

- **Demonstrations.** For example, demonstrating that the functional safety requirements have been correctly implemented.
- **Checklists.** For example, to ensure that EM design measures have been observed, applied and implemented correctly. Checklists encapsulate an organisation's experience, and help to retain important real-world knowledge despite turnover in personnel.
- **Inspections.** For example, checking that assembly and installation have followed the EM design requirements correctly.
- **Reviews and Assessments.** These ensure compliance with the objectives of each phase of the lifecycle. Usually performed by experts, on each phase of the lifecycle and the activities within them.
- **Audits.** These include checking that the correct specification, design, assembly, installation and verification processes have been followed.
- **Non-standardized checks and tests.** There are very many non-standard EM checks and tests that can (and often should) be done to improve confidence in safety integrity. They are often quick and low-cost.
- **Individual and/or integrated hardware tests.** Different parts of the safety system are assembled step-by-step, with checks and tests applied to ensure that they function correctly at each step.
- **Validated computer modelling.**
- **EM testing** (e.g. factory acceptance test or on-site testing). An EM test plan should be created for each design of safety system, based upon the knowledge that has been gained during the above work. The test plan should depend upon the anticipated worst-case EM environment, and the way in which the design has been realised.
- **Physical testing.** Appropriate highly accelerated life tests should be applied, at least to the critical design elements, to verify that the EM performance would be adequate for the anticipated lifetime. This might not be required where a particular design technique has already been proven to be adequate for the foreseen lifecycle environment.

The issue of verification/validation is not discussed further here. It is hoped that it will be the subject of a future article.

3. Verification and validation of the final system assembly / installation

This is a Quality Control (QC) issue, and employs many of the design verification and validation techniques briefly described above. The aim is to ensure that the achievement of adequate EM and physical performance over the lifecycle is not compromised – for example by substandard workmanship, materials, or equipment.

In the case of one-off safety systems, verifying/validating the final system will often be the same thing as verifying/validating its design.

An issue not covered above is verifying the final system's EM and physical environments, where the design was based upon estimates. If the estimates turn out to be too conservative, design/assembly/installation modifications might be required.

It is hoped that these issues will be covered in more detail in a future article.

4. Operation, maintenance, repair, refurbishment, upgrade and modification

Procedures need to be in place, and enforced, to ensure that the required EM performance is not degraded any more than was anticipated by the design, over the entire lifecycle. In some cases, systems will be designed so that they do not require special activities by their operators, repairers etc. But in other cases certain specified activities may be required.

However, remembering that safe design takes foreseeable use/misuse and faults into account, the design should ensure that any activities by operators, repairers, etc., that could excessively degrade EM performance would result in safe operation (e.g. by limiting certain operational functions, such as slowing the speed of operation of a machine) or safe shutdown.

5. Overall conclusions

EMI-related functional safety cannot be verified, at any reasonable cost or timescale, solely by EM immunity testing. To reduce the safety risks caused by EMI to acceptable levels over the lifecycle, methods similar to those already employed for all other safety issues should be employed – the application of well-proven and well-understood EM and physical environment assessment, design and assembly techniques, plus a number of verification and validation techniques and appropriate QC measures.

6. References for Part 2

[1] RCTA/DO-160E, Civil aerospace EMC standards, from www.rtca.org

[2] MIL-STD-464, "*Department of Defense Interface Standard – Electromagnetic Environmental Effects – Requirements for Systems*"

[3] IEC 61508, "*Functional Safety of Electrical/Electronic /Programmable Electronic Safety-Related Systems*"

[4] "*Specifying Lifetime 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.

This article is based on "*Why EMC Testing is Inadequate for Functional Safety — and What Should be Done Instead*", Keith Armstrong, IET 1st International Conference on System Safety, London, U.K., 6-8 June 2006, ISBN 0-86341-646-2, pp 179-183.

EurIng Keith Armstrong C.Eng MIET is at Cherry Clough Consultants. He may be contacted at: keith.armstrong@cherryclough.com.