Another EMC resource
from EMC Standards

Introduction to EMC for Functional Safety

Helping you solve your EMC problems

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

Introduction to EMC for Functional Safety

Presented at the EMC-UK 2004 Conference, Newbury, UK, 12 + 13 Oct 04

EurIng Keith Armstrong C.Eng MIEE
Cherry Clough Consultants

Summary

This paper addresses a gap in safety and electromagnetic compatibility (EMC) regulations and standards, in the commercial, industrial, transportation, healthcare and many other industries (including security and military).

The gap exists because existing safety and EMC regulations and standards do not correctly address the issue of electromagnetic interference (EMI) from the viewpoint of lifecycle safety ('EMC for Functional Safety').

Where errors or malfunctions in electronics could possibly have safety implications the resulting safety risks can fall right through these gaps, leaving users at risk from unsafe products or systems and manufacturers at financial risk from liability lawsuits, product recalls, and loss of customer confidence.

This is an increasing problem because of the huge increase in the use of electronics (especially computer-based technology) in safety-related applications, and because the developments in electronics that make them more cost-effective also make them more likely to suffer EMI.

This paper briefly describes the problem, and then introduces an engineering method (based on the IEE's guidance document [1]) that deals with EMI correctly to help reduce functional safety risks in a cost-effective manner – over the lifecycle of a product, equipment, system or installation (abbreviated to 'equipment' in the rest of this paper).

Similar 'gaps' appear in regulations and standards for legal metrology, security, military and other areas where high reliability is required in situations where there are no direct safety implications. Only a little adjustment would be required to apply the engineering method introduced here to these areas.

Introduction to the problem

Most safety regulations and standards concentrate their efforts on *intrinsic* safety – the possibility that injury or damage could occur due to electric shock, fire, mechanical instability, sharp edges, etc. In this paper we are concerned with *functional* safety – where the hazards and risks depend upon the correct *operation* of devices, equipment, systems or installations. IEC 61508 [3] is the basic standard covering the functional safety requirements of complex electrical, electronic, or programmable electronic equipment, and requires a quantified risk assessment approach. A number of sector-specific functional safety standards are being developed, based on [3].

Electronic technology is increasingly used where its accuracy or reliability is important for functional safety. This is mainly due to the useful amounts of processing power now becoming available in low-cost digital devices. The accuracy and reliability of such safety-related electronics is a functional safety issue. Unfortunately, *all* electronic technology is inherently prone to suffering from inaccuracy, errors in operation, or even damage, due to EMI.

The electromagnetic (EM) environment of an item of equipment is the totality of all of the electromagnetic disturbances that exist at its operational location. It is generally becoming more 'polluted', due to increased use of electronic technologies, especially wired datacommunications, wireless communications, and switch-mode power conversion. As a consequence, existing equipment designs are more likely to suffer errors or fail.

The integrated circuits (ICs) and transistors used to construct electronic products and systems are becoming more vulnerable to interference and damage from EM disturbances as their feature size decreases, operational speed increases, and operating voltages fall. These developments make their internal electronic signals 'weaker' and more easily corrupted by a given EM disturbance, and that actual damage to their internal structure is more likely.

Software employs electronic signals and ICs, of course, and when they suffer from interference or damage the software can suffer from errors or malfunctions, causing the equipment controlled by the software to suffer errors or malfunctions.

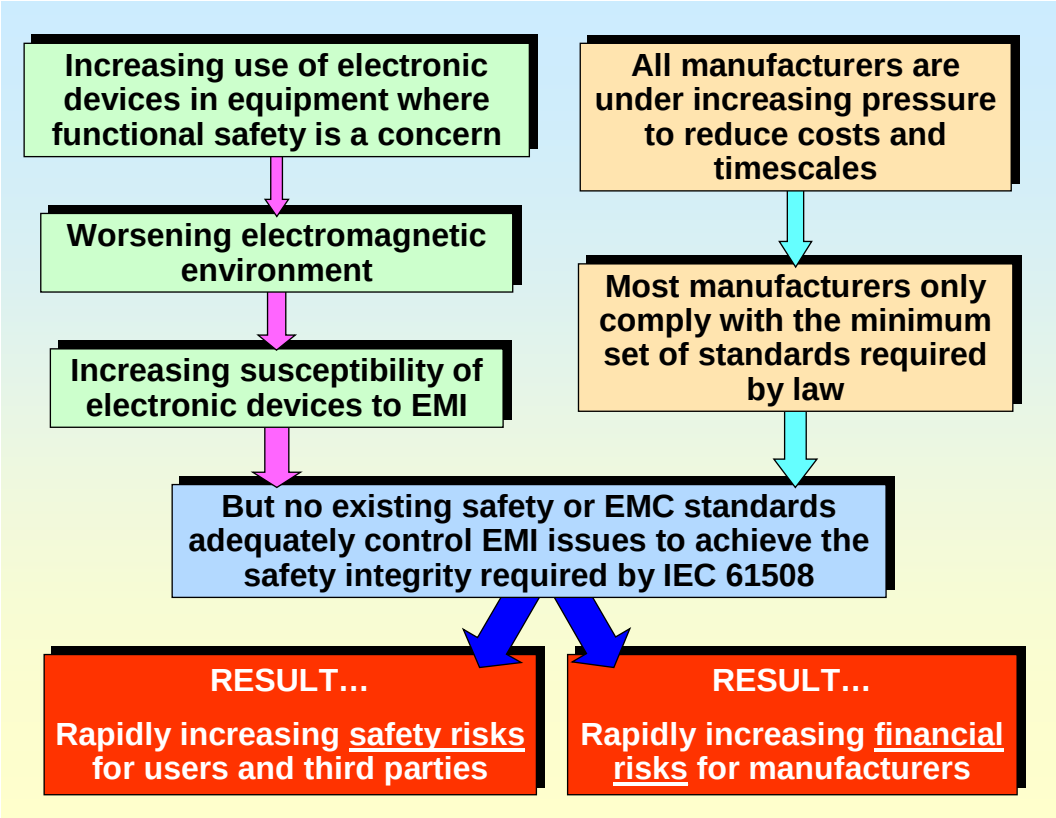
Regulations on EMC are becoming commonplace in many countries around the world – but except for the European Union's (EU's) EMC Directive they generally do not cover EM immunity. However, the EMC Directive's immunity requirements are generally inadequate anyway for EMC for Functional Safety, as I shall show later.

Regulations on product safety are becoming commonplace in many countries around the world. But most (if not all) present-day safety regulations and safety standards provide very poor control of EMC for Functional Safety, as I shall show later.

So, neither EMC nor safety regulations nor standards correctly address the reliability and EMI performance needs of electronics when used in safety-related applications. This is the 'gap' mentioned in the Summary above.

The overall result is that users and third parties are being exposed to increased risks of safety hazards, and suppliers are exposed to higher risks of product liability claims, as shown by Figure 1.

FIGURE 1 Increasing risks due to EMI



Some people assume that all of the hazards are covered by safety standards, so no extra work is needed for EMC. But even if all of the possible hazards were actually covered by safety standards, this approach ignores the fact that inadequate EMC can dramatically change the risks (probabilities) that those hazards will occur, possibly making the health or safety provisions in the existing standards inadequate.

This is best illustrated with an example. There is no backup system for the mechanical steering of a motor vehicle (e.g. rack and pinion, worm and nut, etc.), because although loss of steering can give rise to a very serious hazard, the risks of failure of the traditional steering systems are very low

But do you think a single 'steer-by-wire' electronic system would be just as safe?

The correct answer is *no*, because the reliability of the electronic system is much lower than the traditional mechanical steering system (for example, IEC 61508 would require redundant systems plus special software techniques).

The steer-by-wire example shows that, because equipment is increasingly employing complex electronic technologies both in functional control and safety systems, e.g...

- surgery by robots controlled remotely via the Internet
- 'fly-by-wire' and 'drive-by-wire' technologies
- hazardous plant controlled by computers

…then a detailed hazards assessment and risks analysis is always required for all new designs, instead of simply applying the latest versions of the most relevant safety standards. Some safety standards are decades out of date, in some areas, and all safety standards are out of date on the day they are published, due to the many years that it takes their committees to agree.

IEC 61508 and IEC/TS 61000-1-2

This standard [3] covers the "Functional safety of electrical, electronic and programmable electronic safety-related systems" and is used by the HSE (Health and Safety Executive, UK) as an example of good engineering practice for complex safety-related systems. It has also been adopted as an EN standard (EN 61508) but is not 'notified' or listed under any EU Directives.

[3] requires EMC to be taken into account for safety reasons, although many practitioners (and some authors) seem to be ignoring this. Unfortunately, it contains no *specific* EMC requirements, a lack that IEC 61000-1-2 [4] hopes to make good in due course.

IEC 61000-1-2 is intended to become the IEC's 'basic standard' on EMC for Functional Safety, but at the moment it is not a full IEC standard, but an IEC Technical Specification. Like the IEE's guide, and like MIL-STD-464 it adopts a risk-based approach in its main text, but its examples and appendices rely too much on guessing the EM environment and applying normal (IEC 61000-4-x) immunity testing methods, instead of focussing on good EMC design and assembly techniques and appropriate verification tests. The author is a member of the maintenance team currently working on modifying IEC/TS 61000-1-2 with the aim of making it a full IEC standard in a few years time.

Appropriate methods

The military have a lot of experience in the area of EMC for reliability and functional safety (for example, as expressed in MIL-STD-464 [5]) but they don't (yet) use a quantified risk assessment process such as that required by IEC 61508. Military methods of controlling EMC for safety or mission criticality would be excessive for many manufacturers but they might be quite reasonable for some projects, e.g. commercial passenger transport vehicles or systems (train, plane, etc.) or dangerous plant (e.g. nuclear power).

So this introduction to EMC for Functional Safety is aimed at raising the general awareness, in industry as a whole, so that people can design and implement the procedures that are most appropriate to their business, based on realistic assessments of lifecycle costs and risks and their exposure to liability claims.

The IEE's Guide and training course

The Institution of Electrical Engineers (IEE), based at Savoy Place, London, Great Britain has been concerned with EMC-related functional safety issues for many years. In 1998 they established a working group (WG) to develop some professional guidance on this issue. This WG produced the *"IEE Guidance Document on EMC and Functional Safety*" [1], published by the IEE in September 2000; believed to be the first such guide ever published.

EMC and safety experts from a wide range of industries, along with representatives of the UK's Health and Safety Executive (HSE), were represented on the WG. Care was taken in the composition and management of the WG to ensure that the Guide it produced was relevant to real engineering, safety, and financial issues.

A paper on this IEE guide was presented at the IEEE EMC Symposium in Montreal, August 2001 [6]. The IEE's guide was subsequently employed by the EMC Test Labs Association in their Technical Guidance Notes on the EMC requirements of the Low Voltage and Machinery Safety Directives [7] [8].

The IEE created a training course on "EMC for Functional Safety, Legal Metrology and High-Reliability Systems" in 2004 [2]. It is based on [1], with a great deal of additional material useful for real projects.

The purpose of the IEE's guide [1] and training course [2] is partly to help…

- comply with professional institutions' ethical guidelines
- comply with EU Directives and Health and Safety laws

But their main purpose is to help manufacturers and others to use new technology whilst saving money by reducing financial risks...

- by reducing exposure to liability claims
- by maintaining customer confidence
- by making safety incidents less likely to occur.

Liability

Exposure to liability claims is reduced if the 'state of the art' in safety was applied in the design and manufacture of an item of equipment – and this now includes 'EMC for Functional Safety' issues.

Liability claims can be very costly indeed. There is no limit to the civil damages that can be awarded under the Product Liability Directive (85/374/EEC) in the UK and some other EU member states.

Even a single liability award can be very costly indeed, but loss of customer confidence can cost a great deal more than a liability claim, because it is possible for a company to lose the good reputation it has built up over generations, and for some companies this can be worth billions.

We don't hear a great deal about liability cases because most of them are settled out of court, because the company fears the negative publicity. But safety incidents that attract media attention (such as rail or plane crashes) cannot be kept quiet in this way.

It is often difficult to persuade directors and managers to release the funds and resources needed to do safety-related work correctly. The costs of doing the work can be accurately estimated, but many engineers are uncomfortable with quantifying the benefits to the company of correct safety design. In such situations, engineers need to learn the language (jargon) of financial risk exposure. This easily enables those engineers who are experienced in quantifying safety risks to describe financial cost/benefits to management in terms they understand.

High-reliability, mission-criticality, legal metrology, military and security applications

This paper introduces EMC for Functional Safety – but the methods it describes are also appropriate to high-reliability, mission-critical and legal metrology applications, and also to military and security applications. They just need a little tweaking to replace 'safety hazards' by 'financial hazards' (or other 'hazards' to be risk-reduced).

Achieving high reliability can be much more difficult than functional safety. Safety designers often use 'fail-to-safe' methods such as 'controlled shut-down' and 'emergency stop' which protect human health, but cause downtime (some methods can even damage the equipment). But 'high-rel' or mission-critical equipment often cannot use such methods, and life-support equipment may not be able to either.

Why normal EMC immunity testing methods are inadequate, on their own, for achieving Functional Safety

Safety standards are always based on the use of well-proven safety engineering techniques, which take account of….

- all credible faults
- environmental extremes and ageing
- reasonably foreseeable use, or misuse
- *over the whole lifecycle of the equipment.*

This is quite different from normal EMC immunity testing – which ignores everything to do with the equipment lifecycle. Some safety standards are beginning to add 'EMC for functional safety' requirements, but instead of employing the IEC's (future) basic standard on EMC for Functional Safety, IEC/TS 61000-1-2, they are following the approach used for the safety of medical devices and automobiles instead [9]. They are simply applying EMC immunity tests in much the same way as is done for compliance with the EMC Directive, usually with some sort of 'safety margin' (e.g. 6dB) – despite the fact that this approach is clearly inadequate when dealing with functional safety issues, as shown below.

Normal immunity testing only covers one type of disturbance at a time, whereas in real life equipment is usually subjected to a number of electromagnetic disturbances (threats) simultaneously. Tests have shown [10] that when one disturbance is applied (e.g. a radiated RF field) the immunity to a simultaneous disturbance (e.g. fast transient burst, ESD, etc.) is often seriously compromised.

Normal immunity testing does not simulate real-life EM exposure. Traditional EMC test methods are designed for accuracy and repeatability and do not simulate real-life exposure very well. For example, normal radio frequency (RF) immunity testing uses a single modulation frequency (e.g. at 1kHz) – but an equipment is much more vulnerable to RF threats when they are modulated with a frequency that is close to one of its control frequencies, as real-life threats can sometimes be. This fact is well known to practitioners of electronic warfare.

EMC 'risk analysis' is not normally done for normal immunity testing. "EMC Directive" immunity tests are supposed to simulate the 'normal' EM environment, but…

- they ignore the close proximity of mobile radio transmitters (e.g. walkie-talkies, cellphones, Bluetooth, Wi-Fi, etc.)
- and they ignore almost all EM disturbances at less than 150kHz and 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 overvoltages known to occur annually on normal low-voltage AC supplies in Europe and the USA (due to thunderstorms and reactive load-switching).

See [11] for more on this issue.

Normal immunity testing uses one RF test frequency at a time, but multiple RF threats are not uncommon in real life (e.g. when near a broadcast transmitter, or cellphone basestation) and intermodulation within circuits and equipment will create new noise frequencies inside the equipment. For example, two RF channels at 5.000 and 5.001 GHz will create 1MHz interference inside circuits even when it is 100% shielded and filtered against external 1MHz threats.

Normal immunity testing uses a limited range of transient waveshapes, whereas real-life transient threats can have a wide range of very different waveshapes – hence they expose the equipment to very different frequencies simultaneously. Intermodulation (IM) inside the equipment generates multiple "IM product" frequencies that are almost impossible to predict, with effects that are also difficult to predict.

Normal immunity testing does not simulate foreseeable EM exposure, they only cover 'normal' EM environments, not low-probability EM disturbances or unusual environments. But where high levels of safety integrity are required, even very low-probability risks may be unacceptable – so low-probability EM threats should be considered.

Normal immunity testing might use inappropriate compatibility margins.

All electromagnetic disturbances vary from place-to-place and time-to-time according to some statistical basis. Normal immunity tests set compatibility limits that are appropriate for commercial and industrial reliability, often at the 'two-sigma' statistical level, which corresponds to 95%. For example, IEC 61000-2-2 permits 5% of EM events to exceed the tested levels. But these compatibility levels will probably not be tough enough where safety is a concern, depending on the safety integrity required by the application. Some safety systems will need the confidence that at least 99.9% of EM disturbances do not cause errors or failure.

Faults are not addressed by normal immunity testing. The normal EM activity in an environment must be withstood all of the time, but normal immunity testing does not simulate common faults that can affect EMC, for example….

- a broken electrical connection in a filter capacitor, or in a filter's ground bond, that could ruin the filter's EM performance
- a circuit component that is accidentally short-circuit, open-circuit, out-of-tolerance, or the wrong type or value has been fitted
- a broken spring finger gasket (not an uncommon fault) or broken electrical bond that could ruin the shielding effectiveness of an enclosure.

Normal EMC immunity testing takes no account of the foreseeable physical environment, or ageing. The physical environment of an item of equipment includes exposure to mounting stresses, shock, vibration, condensation, dusts, liquids, ageing, ultra-violet light, temperature extremes and

temperature cycling, corrosion, supply voltage extremes, etc. All of these can all have a bad effect on EM vulnerability [12], for example by…

- reducing shielding effectiveness through poor contact at EMC gaskets
- reducing filtering by ageing of filter capacitors and temperature variations of inductors' values.

Filter performance 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 due to its physical environment has been measured [13].

The performance criteria used for normal immunity testing might be inappropriate for safety purposes. Degraded performance during interference that is considered to be perfectly acceptable for an individual item of equipment might result in unsafe behaviour of the system it is employed in. For example, the IEC 61000-4-4 fast transient burst immunity test allows any amount of performance degradation *during* the test – so it is not uncommon for the d.c. output of a power supply unit to collapse to zero during a burst. The d.c. power supply manufacturer can claim that his unit fully meets IEC 61000-4-4, but when it is used to power a circuit (especially microprocessor) the system as a whole can fail the IEC 61000-4-4 test, due to a microprocessor's software crashing, due to the DC power supply's performance.

So the performance criteria for the individual items of equipment – when they are tested for immunity to EMI – depend upon the specific application. They must satisfy the needs of the final safety system as identified by a hazard assessment and risk analysis [11].

Only a representative sample is tested for EMC

Most companies design their equipment, test it using 'black box' EMC test methods, then modify it as required until it passes its EMC tests. But most of them have no real idea whether the final version passed because of good design, or because of a fluke that might not be repeated in future manufacture.

Maybe an altered cable routing or a different batch of ICs would make the EMC performance worse? Many companies introduce 'small' changes in production, software 'bug fixes', and substitute components – without re-qualifying EMC – and many don't routinely test EMC in serial manufacture either, so they have no real knowledge of the actual EM performance of the items of equipment they supply to their customers.

Compare this with the approach typical of safety standards, which require testing of the basic safety features of *every item of equipment manufactured*, and a pass result documented for every item supplied to a customer.

The fact that an item of equipment once passed an EMC immunity test proves nothing at all about the quality of its EM design, or the EM immunity performance of the items actually supplied.

EMC testing does not address maintenance, repair, refurbishment, upgrades (e.g. software)

In real life, equipment is subject to cleaning, maintenance, repair, refurbishment and upgrades. Safety test standards take some of these issues into account as a matter of good safety engineering practice – but no EMC testing standards do.

Safety requires good EMC techniques in design, assembly and maintenance

Safety over the lifecycle of an equipment requires the use of good EMC techniques in design, assembly, QA and maintenance – in the same way that well-proven safety design methods are required for all other safety issues, including software (see IEC 61508-3 [14]).

EMC testing is necessary for verifying the EMC design techniques that were used (or are to be used), but the normal "EMC Directive" test methods (e.g. the IEC 61000-4-x series) are inappropriate on their own. Special test methods are required, which take the foreseeable EM and physical environments into account. For more on the inadequacy of normal EMC immunity testing (including that used for automotive, rail and medical safety) and what should be done instead when verifying EMC for Functional Safety see [15] and [16]. [2] has a lot of detail on this issue.

Safety shortcomings in EU EMC directives and their standards

The **EMC Directive** (EMCD) does not cover safety. EMC for functional safety is covered by safety directives instead, see CENELEC R0BT-004:2001 and [6].

The **Radio and Telecommunication Terminal Equipment Directive** (R&TTE) does not cover safety-related communications systems

The various **road vehicle EMC Directives** (e.g. 95/54/EC) are inadequate for EMC-related functional safety because they rely solely on normal immunity testing methods.

The **EN 50121 series of railway EMC standards** also rely solely on normal immunity testing methods.

The following EMC immunity standards notified under the EMC Directive all state that they *do not cover safety issues.* Most of them also state that they do not cover the close proximity of hand-held radio transmitters, even though this is now a normal part of the EM environment.

- EN 61000-6-1 (generic immunity for the residential commercial and light industrial environments)
- EN 61000-6-2 (generic immunity for the industrial environment)
- EN 55024 (information technology and telecommunications)
- EN 61326-1 (measurement, control, and laboratory equipment)
- EN 50130-4 (security systems).

EMC shortcomings in 'CE marking' EU safety directives and their standards

All the 'New Approach' EU directives are considered to be 'Total Safety' directives, and this is made clear in their 'essential requirements' Articles.

EN standards notified (listed) under these Directives are supposed to deal with all of their essential requirements, but they usually do not cover all possible safety issues – so additional testing, skills or expertise may be required to fully comply with the directive's essential safety requirements.

Compliance with a "CE marking" EU Directive requires…

- a declaration about the conformity assessment (usually based on testing to notified safety standards)
- and a declaration that the essential safety requirements are complied with.

So each design requires a thorough analysis of the hazards and assessment of the risks, with the results checked against the most relevant harmonised standards to see if any hazards/risks need additional standards, or skills or expertise, to be applied.

Most manufacturers assume that all they have to do to comply is test to the most relevant standard(s), and most test laboratories encourage this error. But where a safety incident has occurred, official investigators will be looking for evidence of good safety engineering practices, such as the use of hazards and risks assessments to guide design and verification to help ensure the equipment really is safe, and doesn't 'slip through the gaps' in the usual test standards.

Medical equipment is covered by one of the following…

- the Medical Devices Directive: 93/42/EEC
- the Active Implantable Medical Devices Directive: 90/385/EEC
- the In-Vitro Diagnostics Directive: 98/79/EEC

For all three of them, the relevant standard for the EMC-related safety of medical devices and equipment is EN 60601-1-2. But this standard relies on normal immunity testing methods, using IEC 61000-4-x standards with EM threat levels which could easily be exceeded in real-life, and does not test at all for some common EM threats. Also, its immunity tests and test levels are almost identical to those used by the EMCD's immunity standards – which state that they do not cover safety.

EN 60601-1-2 does not employ quantified risk analyses, as required by IEC 61508 for safety-related systems, and the 2002 version allows manufacturers to pass significant responsibility for the EMC-related safety of their medical equipment on to the user. This seems to assume that all healthcare premises employ the necessary EMC expertise and resources to fully manage their EM environments on a day-to-day basis – which is very far from the real situation.

The Low Voltage Directive (LVD, 73/23/EEC amended by 93/68/EEC) does not even mention functional safety at all, much less 'EMC for Functional Safety', so some manufacturers assume that it does not cover this issue. But the LVD does cover EMC for Functional Safety, because it is a 'total safety' directive. The result is contradictory guidance from experts and Notified Bodies.

Two well-known safety standards that are notified under the LVD are…

- EN 60950:2000 (computers and telecoms)
- EN 61010-1:2001 (measurement and control)

…but they both state that they do not cover functional or performance issues.

EN 60335-1 (household appliances) *does* cover functional issues, but has no requirements for preventing EMI from creating safety problems. There is an amendment under discussion which would add a few normal EMC immunity tests, to a subset of possible operational conditions, which (as shown above) is inadequate. Why does it not apply the same safety-engineering design-based approach to EMC, that it applies to all its other safety issues?

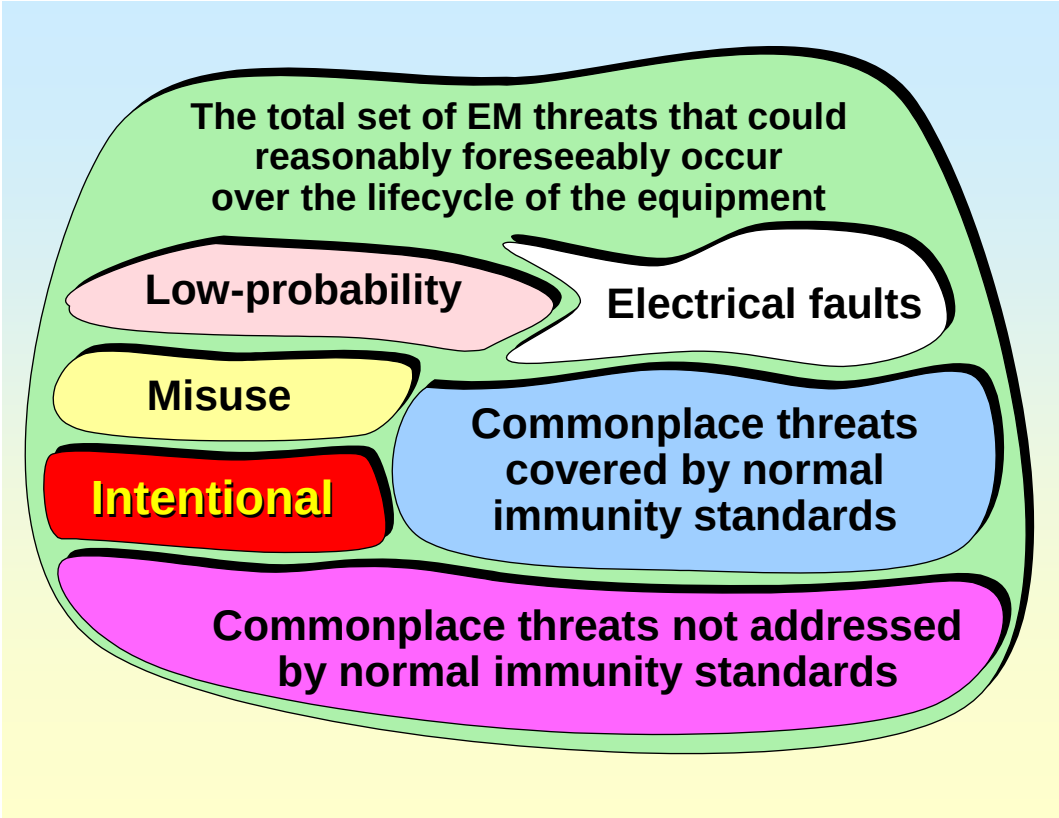
The Machinery Directive (98/37/EC) and its notified standards *attempt* to cover 'EMC for functional safety', but does so only in the most general terms and fails to be explicit about what work it really requires.

One of the most relevant Machinery Directive safety standards is EN 60204-1 (electrical equipment of machines). This *tries* to cover EMC for Functional Safety – but is not comprehensive – and in the end simply refers to EMC Directive immunity standards despite the fact that they state in their text that they do not cover safety issues (see above).

EN 954 (machine control systems) does not address electronics at all. It has no EMC requirements for the electromechanical control systems that it does cover – despite the fact that they are not immune to all EM disturbances and have particular problems with supply dips, dropouts and interruptions, and with surge overvoltages and overcurrents.

The result of all this is contradictory guidance from machinery safety experts and Notified Bodies, as shown by Figure 2.

FIGURE 2 Conflicting EMC guidance from machinery safety experts



There are many other EU safety directives, such as for **Potentially Explosive Atmospheres**; **Personal Protective Equipment**; **Gas Boilers**; etc., but despite the fact that the functional safety of the equipment they cover often, these days, depends upon the correct functioning of electronics – they make little (or no) mention of EMC at all, leading people to believe that all EMC aspects, including safety, are covered by the EMC Directive (which they are not, as described earlier).

The **Measuring Instruments Directive** (MID, 2004/22/EC) is not concerned with safety at all, but it is concerned with legal metrology. It is quite robust in requiring that EMI does not affect measurements,

but it doesn't use words like foreseeable and it doesn't specify how the EM environment is to be assessed – and therein lies a problem.

It specifies three EM environments: the first two basically equivalent to the two types of generic EMC standards; with a third for vehicular applications. It doesn't say which EMC standards apply but people are going to turn to the IEC series, which of course only specify the 'normal' environments and not reasonably foreseeable extremes. So I'm sure that manufacturers will tend to treat the immunity of equipment covered by the new MID just as they would for the EMC Directive, since it gives them no guidance on how to assess foreseeable EM environments – or what to do to ensure reliable accurate measurements if they had that EM knowledge anyway.

How EMC should be controlled for functional safety

Now that the problem has been briefly explained, it is time to introduce the solution.

The IEE's Guide [1] and associated training course 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?

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

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

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

These six activities will now be briefly described…

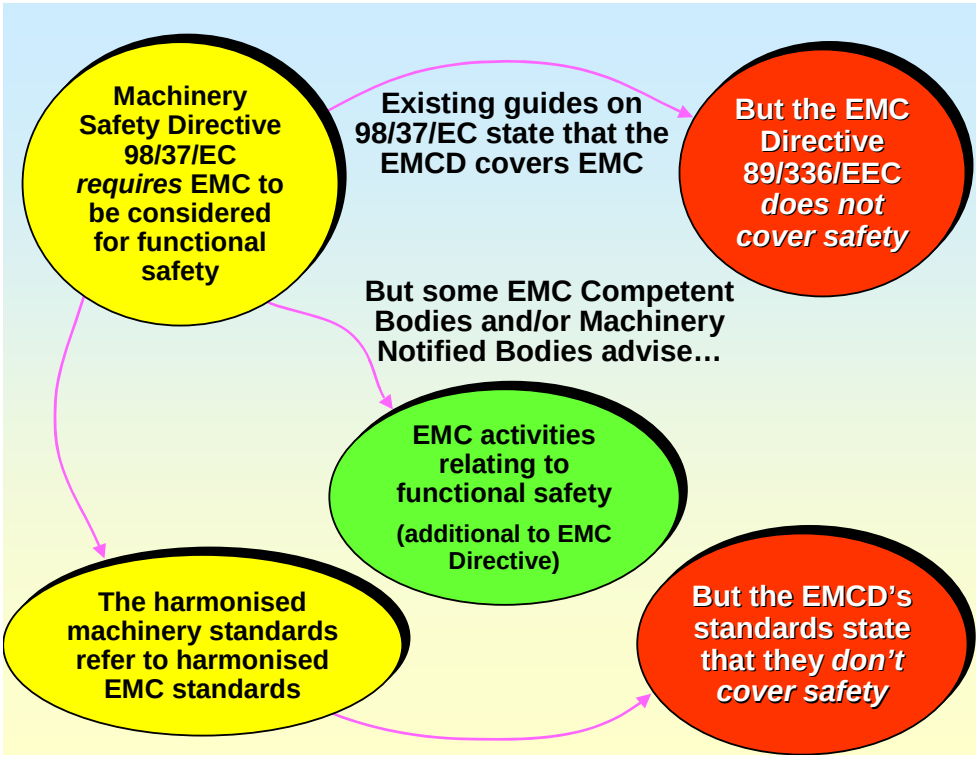
A) What EM threats could the equipment (foreseeably) be exposed to?

EM 'threats' are more correctly called EM disturbances, or EM phenomena. EMI is what happens when the equipment is not compatible with its EM environment – i.e. when EMC has not been achieved in real life, over the equipment's lifecycle.

An 'EM threat assessment' is required for the foreseeable EM environment of the equipment's intended operational site, taking into account low-probability EM threats over the lifecycle of the equipment. Figure 3 gives an overview.

There is a lot of published information on various EM environments, but it is rarely gathered in one place. [17] is a useful resource.

FIGURE 3 Assessing foreseeable EM threats



B) What could (foreseeably) go wrong ?

Electromechanical devices can malfunction and/or be damaged, and this is especially a problem for (so-called) 'hard-wired' safety systems.

Analogue circuits can suffer erroneous signals and/or be damaged, and this is especially a cause of errors in instrumentation.

Digital circuits and programmable devices can change operational mode, malfunction, and be damaged, especially a problem for control and automation.

All of these possibilities should be considered in the hazards assessment and risk analysis.

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 of A-C above?

This should take into account the severity of the possible safety hazard, and the scale of the risk. It is best to employ the quantified risk assessment approach of [3], remembering that exposure to EM disturbances, and the equipment's responses to those EM 'threats', both have statistical probabilities. It is a bit like predicting the "100-year" gale or wave.

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

Five kinds of actions are needed, and they should be 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.

E2) EMC risk-reduction by design

The EMC performance of each of the safety functions should be designed to be sufficiently reliable over the equipment's whole lifecycle, using the 'Safety Integrity Level' (SIL) approach described by [3].

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.

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

EM 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).

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.

E5) Maintenance of safety performance despite modifications and upgrades

A Quality Control (QC) procedure 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 and verification activities over the "equipment's lifecycle" should take into account…

- manufacture
- storage
- transport
- installation
- commissioning
- operation
- maintenance
- repair
- refurbishment
- decommissioning
- disposal.

An incremental process is required. Achieving the necessary confidence in EMC for Functional Safety should be a continuing 'incremental' process throughout the whole project. This should create an 'audit trail' that shows how confidence is built throughout research, design, development and final verification…

- showing that the safety functions of the final design will satisfy their performance requirements in the foreseeable EM environment, with the required reliability for their level of safety integrity
- initial engineering design should be based on analysis, models and previous experience
- as hardware and software become available, testing (of components and subsystems) should validate the analysis and models used
- testing is often necessary to obtain information not amenable to determination by analysis
- the design evolves as better knowledge is achieved
- finally, whole system testing and follow-on analysis completes the incremental verification process.

As soon as 'EMC testing' is mentioned, most EMC engineers immediately tend to think of anechoic chambers and formal test methods – then wonder how these can be applied to components and subsystems.

But EMC testing to verify design aspects can often use very simple test methods, which may need to be designed to suit whatever it is that is being verified.

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, and…

- 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.

Although [4] does not *yet* represent the 'state of the art' (see earlier), nevertheless, it is recommended to apply this standard on all safety-related equipment – whilst also heeding the guidance of the IEE's training course on EMC for Functional Safety. Because [4] is the most relevant international specification for EMC for Functional Safety, applying it will help to show 'due diligence' and may help deflect any liability claims.

References

[1] *'IEE Guide to EMC and Functional Safety'*, IEE September 2000, available for free download from http://www.iee.org/Policy/Areas/Emc/index.cfm as a 'Core' document and nine 'Industry Annexes', in either Word or PDF formats.

[2] EMC for Functional Safety, IEE (London, UK) training course (first held February 10th 2004), http://www.iee.org.uk, contact abennett@iee.org.uk for its 2005 dates.

[3] IEC 61508 *'Functional safety of electrical/electronic/programmable electronic safety-related systems'* (in seven parts). This is a voluntary standard which (it is understood) might not be adopted by the EU as an EN, or become a harmonized standard under any directives. However, it will influence some product standards which could become EN's and might become harmonized. It is now being used by the UK's Health and Safety Executive as an example of good safety engineering practice.

[4] 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'*

[5] MIL-STD-464, *'Department of Defense Interface Standard – Electromagnetic Environmental Effects – Requirements for Systems'*, typing MIL-STD-464 into the Google search engine quickly finds sites for free downloads.

[6] *'New Guidance on EMC-Related Functional Safety',* Keith Armstrong, 2001 IEEE EMC International Symposium, Montreal, Aug. 13-17 2001. Proceedings: ISBN 0-7803-6569-0/01, pp. 774-779.

[7] *'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.

[8] The EMC Test Labs Association (EMCTLA), http://www.emctla.co.uk contact Dave Imeson (Secretary) dimeson@iee.org. The EMCTLA is an international association of test laboratories, and has been publishing their helpful technical guidance notes (TGNs) on their website for many years.

[9] *'Review of Progress with EMC-Related Functional Safety'*, Keith Armstrong, 2003 IEEE EMC Symposium, Boston, August 18-22 2003, Proceedings pp 454-459, CD-Rom: ISBN 0-7803-7836-9; Softcover: ISBN 0-7803-7835-0.

[10] *'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.

[11] *'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

[12] *'The Case for Combining EMC and Environmental Testing'*, W H Parker, W Tustin and T Masone, ITEM 2002, www.rbitem.com, pp 54-60.

[13] *'EMC Performance of Drive Application Under Real Load Condition'*, F Beck and J Sroka, Schaffner EMV AG application note, 11th March 1999.

[14] IEC 61508-3, *Functional Safety of Electronic/Electronic/ Programmable Electronic Safety-Related Systems – Part 3: Software Requirements*

[15] *'Why EMC Immunity Testing is Inadequate for Functional Safety'*, Keith Armstrong, 2004 IEEE EMC Symposium, Santa Clara, August 9-13 2004.

[16] *'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.

[17] *'Assessing an Electromagnetic Environment'*, Keith Armstrong, available from Cherry Clough Consultants, phone +44 (0)1457 871 605 or email keith.armstrong@cherryclough.com.

EurIng Keith Armstrong C.Eng MIEE
Partner, Cherry Clough Consultants
Cherry Clough House, Denshaw, OL3 5UE, UK, http://www.cherryclough.com
Phone: +44 (0)1457 871 605, Fax: +44 (0)1457 820 145, e-mail: keith.armstrong@cherryclough.com