



Another EMC resource
from EMC Standards

EMC for functional safety

Helping you solve your EMC problems



EMC for functional safety

Euro-Eng Keith Armstrong, Cherry Clough Consultants*

Electronic technologies are increasingly used in equipment that has an impact on safety. Unfortunately, all electrical and electronic technologies are inherently prone to suffering inaccuracy, errors in operation, or damage, due to electromagnetic interference (EMI).

The electromagnetic environment that equipment is exposed to is generally becoming more 'polluted', due to increased use of wired datacommunications, wireless communications, digital processing and solid-state power conversion. So existing designs are more likely to suffer errors or failures due to EMI.

The internal feature sizes of the integrated circuits and transistors used in electronic equipment are continually decreasing, while their speeds are increasing and operating voltages falling. So new designs are more likely to suffer errors or failures due to EMI.

Software runs on electronic circuits, so when they suffer EMI the software can suffer from errors or malfunctions, causing the equipment controlled by the software to suffer as a result.

Existing standards for equipment safety and EMC do not deal adequately with EMC for functional safety and there are increasing pressures on manufacturers to shorten design/development times and reduce prices.

The overall result, as shown by Figure 1, is that users and others are exposed to increasing safety risks, and equipment manufacturers and employers are exposed to higher financial risks.

Liability issues

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 Britain and some other EU 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 in some cases 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 one of the parties fears negative publicity. But safety incidents that attract media attention (such as rail or plane crashes) cannot be kept quiet in this way.

Legal metrology

This article introduces EMC for functional safety — but the issues it describes are also relevant for high-rel and legal metrology applications and also for military and security applications.

It just needs a little tweaking to replace 'safety risks' by 'financial risks' (or whatever is to be risk-reduced).

Safety designers often use 'fail-to-safe' methods such as 'controlled shut-down' and 'emergency stop' that protect human health but cause down time. But 'high-rel', mission-critical, legal metrology equipment often cannot use such methods and equipment used for life-support and some security applications may not be able to either.

So achieving adequate reliability can be more difficult than achieving adequate functional safety.

Conventional approach inadequate

Safety standards employ well-proved safety engineering design and verification techniques that take into account foreseeable...

- Faults;
 - Environment, environmental extremes, ageing;
 - Use, misuse
- ... for the whole life cycle of the equipment.

But the conventional approach to EMC never uses the world 'foreseeable' and is based solely on applying a set of EMC performance tests to a new item of equipment in a benign physical environment. This is not an appropriate methodology where safety is concerned.

For example:

- The RF modulation frequency can be critical — but only 1 kHz is used (and 0.5 Hz for some medical equipment);

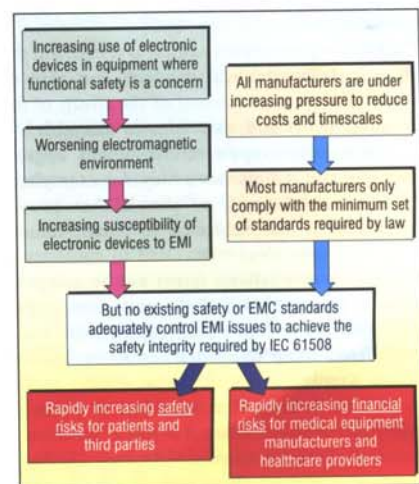


Figure 1: Increasing risks due to the increasing likelihood of EMI.



• In real life, equipment is subjected to multiple EM threats simultaneously (eg, a radiated field plus a conducted mains transient). But conventional EMC testing only applies one threat at a time, which overestimates the equipment's real-life immunity.

Real-life EM exposure might not be tested. Conventional immunity tests ignore foreseeable EM threats, for example:

- Close proximity of mobile radio transmitters (warning signs cannot stop all mobile phone use;
- Almost all EM threats below 150 kHz, and above 1 GHz (2.5 GHz for medical equipment);
- The ± 6 kV (approx) overvoltages that occur on normal 115/230/400 V single-phase AC mains supplies.

Compatibility levels may be too low. Each EM threat varies statistically and conventional immunity tests use 'compatibility levels' that cover most of their range. But 'most' might not be good enough for some applications.

Foreseeable faults are not addressed. The following examples of commonplace faults can badly affect the performance of shielding, filtering or surge suppression:

- Poor connection, short circuits;
- Missing or damaged conductive gaskets;
- Missing or loose fixings.

Foreseeable effects of the physical environment are ignored. For example:

- Filters can be badly affected by high temperatures, supply voltages, and load currents;
- Mounting stresses, shock, vibration, temperature extremes, exposure to liquids, conductive dusts, etc can all degrade the performance of shielding and filtering — as can ageing due to temperature cycling, humidity corrosion, wear and tear, etc.

Only a representative sample is tested. But the EMC performance of supposedly identical products can vary significantly if their design did not take account of the effects of foreseeable tolerances in components and variations in assembly.

Maintenance, repair, refurbishment, upgrades, etc are ignored. Cleaning and maintenance may, for example, require the opening or removal of doors or panels that provide shielding. Real equipment is also subjected to repair, refurbishment, modifications and upgrades.

Performance criteria might not be acceptable for systems. It is usual to assume that if all the units comprising a system pass their EMC tests, the system will have good EMC. But performance criteria considered acceptable when testing an individual unit (eg, a DC power supply) might not be acceptable in a system.

IEC/TS 61000-1-2 is intended to cover EMC for functional safety but at the moment it is just a 'technical report' — not a full standard — and it remains to be seen whether it will become good enough to address these issues.

Safety requires good techniques

Achieving adequate levels of functional safety over an equipment's lifetime requires the use of good EMC techniques in design, assembly, QA and maintenance — in the same way that well-proved design methods are required for all other safety issues, including software.

EMC testing is necessary for verifying the EMC design and the assembly quality in serial manufacture — but the conventional immunity tests may be inadequate and special test methods may be required.

Shortcomings in the EU's directives

The EMC Directive does not cover safety. EMC for functional safety is covered by safety directives instead (see Cenelec ROBT-004:2001).

The following EMC immunity standards notified under the EMC Directive all state in their texts that they do not cover safety issues. Most of them also state that they do not cover the close proximity of portable radio transmitters — even though this is now a normal feature in most real-life EM environments.

- EN61000-6-1 (generic: residential commercial and light industrial environments);
- EN61000-6-2 (generic: industrial environments);
- EN55024 (information technology and telecommunications);
- EN613261 (measurement, control and laboratory equipment);
- EN50130-4 (security systems).

The Radio and Telecommunication Terminal Equipment Directive (R&TTE) does not cover safety-related communications systems and the EMC test standards listed under it rely on conventional immunity testing methods — so they are inadequate for functional safety for the reasons given earlier.

The same problems with inadequate test methods apply to the various road vehicle EMC Directives (eg, 95/54/EC), and also to the railway EMC standards in the EN50121 series.

Compliant with a 'new approach' EU safety directive (ie, one that requires CE marking) means more than simply com-

plying with the relevant EN standards — it also requires that all a directive's 'essential safety requirements' are complied with.

This means that each design requires a thorough analysis of the hazards and assessment of the risks, with the results checked against the safety standards to see if any additional standards, skills or expertise need to be applied to comply with the directive's essential safety requirements.

EMC for functional safety is one example of an area where the existing safety standards are inadequate, and additional expertise is required. For example, two very well-known safety standards listed over the Low Voltage Directive are:

- EN60950 (computers and telecoms);
- EN61010-1 (measurement and control).

They both state that they do not cover functional or performance issues — so they don't cover any aspects of functional safety.

EN 60335-1 (household appliances) does cover functional issues and a recent amendment added a few conventional EMC immunity tests, which are inadequate for EMC for functional safety.

The Machinery Directive and its listed standards attempt to cover EMC for functional safety but do so only in the most general terms and fail to be explicit about what is really required.

A relevant machinery safety standard is EN60204-1 (electrical equipment of machines). This tries to cover EMC for functional safety — but is not comprehensive. In the end it simply refers to immunity standards listed under the EMC Directive, despite the fact that they say they do not cover safety issues.

EN954 (machinery control systems) covers electromechanical (hard-wired) control systems and has no EMC requirements — despite the fact that such systems are not immune to all EM disturbances. The result of all this is contradictory guidance from machinery safety experts and notified bodies.

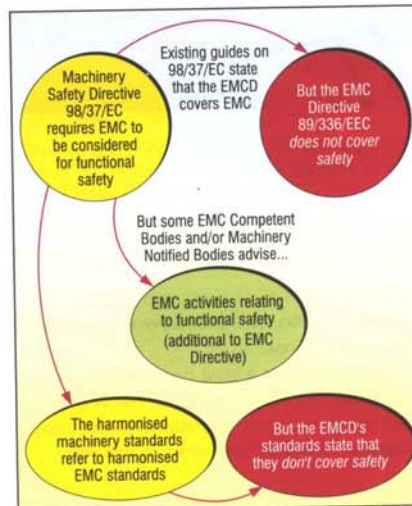


Figure 2: Conflicting EMC guidance from machinery safety experts.

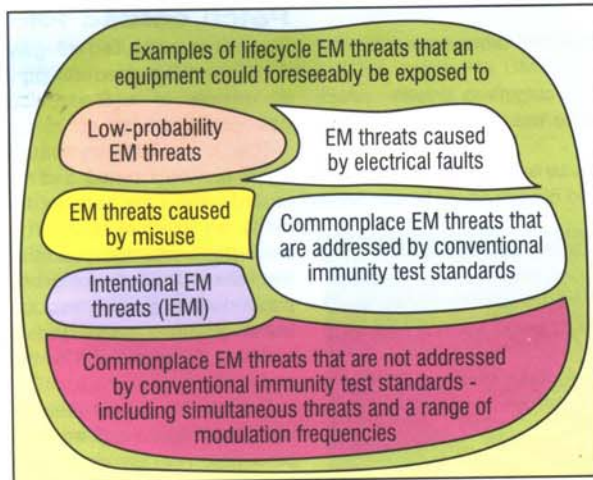


Figure 3: Some foreseeable EM threats.

EMC issues under the three Medical Device Directives are covered by EN60601-1-2, plus any additional or modified EMC requirements in the EN60601-2-x series. EN60601-1-2 is the European harmonised version of IEC 60601-1-2, which is used worldwide for EMC for medical equipment.

It has usually been assumed that both EN and IEC 60601-1-2 cover EMC requirements for safety purposes, but Amendment 1 (September 2004) to IEC 60601-1-2:2001 makes it clear that it does not. Amendment 1 states that for issues of EMC for functional safety, medical devices should apply IEC 61000-1-2 instead.

There are many other EU safety directives, such as Potentially Explosive Atmospheres; Personal Protective Equipment, Gas Boilers. But despite the fact that the functional safety of the equipment they cover often depends on the correct functioning of electronics — they make little (or no) mention of EMC at all.

This leads manufacturers of equipment covered by these Directives to rely on complying with the EMC Directive — which does not cover any safety issues.

The MID is concerned with legal metrology, not safety. It has very strong requirements for EMI not to affect measurements — but it does not say how to achieve this.

The result is that manufacturers are applying the EMC standards listed under the EMC Directive. But these are quite inadequate for ensuring reliable measurements in real life, for their whole life cycle.

Worldwide problem

IEC standards are the basis for immunity regulations and/or standards over much of the world, including Australia and New Zealand. But all the earlier comments about the inadequacy of EN standards where EMC for functional safety is concerned also apply to the IEC standards they are derived from. So although the above discussion focused on European directives, the same problem arises worldwide.

IEC 61508 is the basic standard on functional safety. It covers EMC threats but does not say how they should be dealt with.

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

An 'EM threat assessment' is performed for the foreseeable EM environment of an equipment's operational site(s), taking into account low-probability EM threats over its life cycle, see Figure 3. Provides some useful guidance.

B) What could the EM threats foreseeably affect?

Electromechanical devices can malfunction or be damaged. Analog

and power conversion circuits can suffer errors or be damaged. Digital circuits, programmable devices and software can change operational modes, malfunction, or be damaged. Communications can fail. Data can be corrupted or lost. All these possibilities should be considered in an equipment's hazards analysis and risk assessment.

C) Foreseeable effects of equipment emissions

Conventional EMC emissions standards do not protect nearby radio receivers or other sensitive circuits. So the foreseeable effects on existing equipment of the emissions from the new equipment should be considered.

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

This should take into account the severity of the safety hazards, their probabilities (risks) and the number of people exposed. Remember that EM threats have statistical variations. Errors and failures due to EMI are systematic, not random, and this affects how they must be treated in the equipment's design.

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

Five kinds of actions are needed, carried out in the following order:

- (i) Hazard and risk reduction by design. Design so that the hazards are less severe, the risk is reduced and fewer people are exposed;
- (ii) EMC risk-reduction by design. Electrical and electronic devices, circuits and software that could have a safety impact should be designed to be sufficiently reliable over their life cycle. This should take into account the foreseeable EM, physical and climatic environments; plus use/misuse, wear and tear, ageing, etc;
- (iii) Verification of the design techniques employed. Verification, including EMC testing, should prove that the design meets the specifications resulting from the above work. Special immunity test techniques may be required;
- (iv) Maintenance of safety performance in serial manufacture, maintenance, repair. A quality assurance system should control all the aspects of manufacture that could affect any EM-related safety issues. Sample-based EMC testing will generally be required during series manufacture;
- (v) Change control. A QA system should control EMC safety issues in modifications and upgrades.

F) What documentation is required to show due diligence?

Project records should show that the above steps were carried out in full and that the required EMC performance was determined and 'designed-in' for everything that could have a safety impact from the start of a project and verified at the end. The QA program should also be monitored and its effectiveness recorded.

The conventional approach to EMC cannot give confidence that adequate levels of functional safety will be maintained over an equipment's life cycle.

Instead, good EMC design practices are required to address the equipment's real-world EM, physical, climatic, use/misuse and 'wear-and-tear' environments; design verification may require special immunity tests; and certain QA activities are required.

*Keith Armstrong will be visiting Australia-New Zealand in February-April 2006 to present a series of EMC courses to industry and the public, sponsored by EMC Technologies.

The courses will be presented in each capital city around Australia, plus Auckland and Christchurch, and will be presented in convenient modules ranging from introductory to advanced level. They all use plain English and simple mathematics to describe practical methods proven to have great benefits for quickly achieving EMC at low cost. There will be an emphasis on emerging EMC and signal integrity design challenges associated with the latest types of ICs and co-located wireless data communications.

www.cherryclough.com

Australian agent — EMC Technologies

www.emctech.com.au