EMC STANDARDS

Another EMC resource
from EMC Standards

Introducing the IEE's draft guidance document on EMC and functional safety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

Introducing the IEE's draft guidance document on EMC and functional safety

Eur Ing Keith Armstrong C.Eng MIEE MIEEE
Partner, Cherry Clough Consultants, www.cherryclough.com
Chair of IEE Working Group on EMC and Functional Safety
Phone:01457 871 605 Fax: 01457 820 145 Email: karmstrong@iee.org

1 Background to the IEE's Working Group

Where the correct functioning of an electronic apparatus is important for safety reasons, its electromagnetic (EM) performance with respect to immunity from (and emissions of) EM disturbances can have important safety implications.

Fully complying with the Electromagnetic Compatibility Directive (EMCD) and/or its harmonised EMC standards does not necessarily mean that EMC-related functional safety issues have been properly engineered. This view is now widely accepted, for instance by the European Commission's DGIII, and also by their EMC-SLIM Working Group creating the 2nd edition EMCD.

What prompted the Institution of Electrical Engineers (IEE) to set up a Working Group (WG) to produce a Professional Guidance Document on the relationship between EMC and Functional Safety, was the observation that most design engineers and managers in a wide range of industries thought that meeting the EMCD was all they had to do on EMC. This misperception seemed to be especially true of machinery manufacturers and also of some of the companies who advised them on the Machinery Safety Directive 89/392/EEC (now replaced by 98/37/EC).

Unlike the draft IEC 61000-1-2 these IEE guidelines are not intended to be used as a standard, and they are not prescriptive.

For many people, the acronym 'EMC' means simply the EMC Directive or other EMC regulations such as those applied by the FCC in the USA. Also, when talking about EMC-related functional safety, many people think that EM immunity is the only concern, whereas emissions also need to be taken into account. Although EMC is really the correct term to use, because of the possibility of misunderstanding I try to use the phrase '**EM performance**' instead, when discussing functional safety.

The IEE's WG was quite large, at 18 people. It included acknowledged EMC and Safety experts from a wide range of industries, and also very senior personnel from the UK's Health and Safety Executive (HSE).

The aim of these IEE guidelines was to introduce how best to deal with EM performance where functional safety issues are involved, and they are intended to be used by both engineers and their managers. Because of the traditional differences between EMC and safety practitioners, these IEE guidelines are also intended to help either side bridge the gap to the other.

The WG started work in September 1998, and finished the first full draft of these IEE guidelines in early 2000. At the time of writing these draft guidelines are going through their final approval procedure at the IEE.

2 EM performance is increasingly important, because...

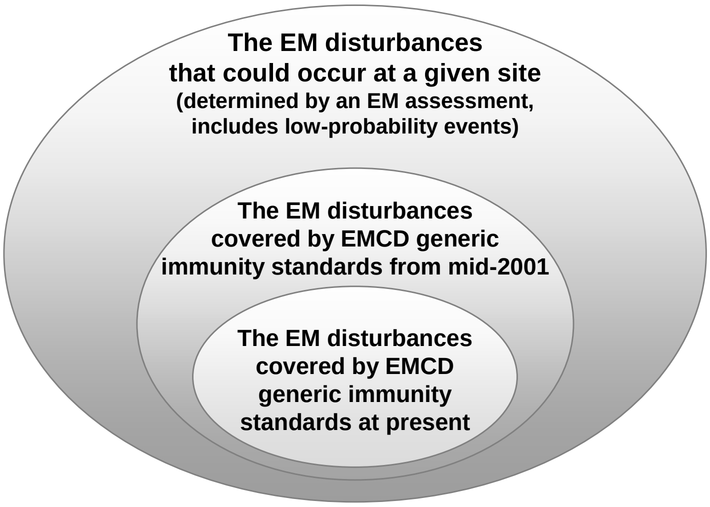
- Mobile radio transmitters (e.g. cellphones, walkie-talkies) are now used everywhere, creating powerful radio-frequency (RF) fields within a metre or so of their antennas.
- Modern electronics technologies (e.g. digital processing, switch-mode power conversion) emit more EM 'pollution' as an accidental consequence of their design and operation.
- Semiconductor chips or ICs use ever-smaller physical features, and consequently are more likely to suffer damage or mis-operation due to EM disturbances.
- Electronics (especially programmable electronics) will soon be used to control *everything.*

3 Meeting the EMCD is not enough for functional safety

The EMCD is solely concerned with preventing technical barriers to trade in the EU Single Market and *cannot* properly deal with EM performance-related functional safety issues. The EMCD only considers normal operation, whilst safety compliance must consider *reasonably foreseeable……*

- operational and environmental extremes
- low-probability events
- faults in itself and in other apparatus
- human errors and misuse

Also, the EMC test standards which are harmonised under the EMCD are based on 'normal' EM environments, *and their scopes specifically exclude functional safety issues.*



Existing safety legislation generally requires a *safety argument* approach to all the EM performance issues that could possibly have an adverse effect on safety hazards or risks, e.g. for these EU safety Directives –

- Low Voltage Equipment
- Machinery Safety
- Toy Safety
- Gas Appliances
- Medical Devices
- Construction Products
- Personal Protective Equipment
- Product Liability
- General Product Safety
- Health and Safety at Work (various)

For plant or large engineering projects there are some additional UK Regulations that can require EM performance to be included in their safety arguments, e.g.:

- The Provision and Use of Work Equipment Regulations, 1998
- The Offshore Installations (Safety Case) Regulations as amended by the Offshore Installations and Wells (Design and Construction, etc.) Regulations, 1996
- The Offshore Installations (Prevention of Fire and Explosion, and Emergency Response) Regulations, 1995.
- The Control of Major Accident Hazard Regulations, 1999 (COMAH)

Other countries no doubt have similar safety regimes for large projects.

4 The economic argument for these guidelines

The cost saved on large numbers of projects by cutting corners on EM performance-related safety issues can easily be cancelled out by just one safety incident. In fact, the entire reputation of a company, built up over decades, can be lost overnight as a result of a single safety incident. Also, there is the possibility of unlimited civil claims for damages under liability laws, which in both the US and the EU assume the manufacturer is guilty until he proves he is not.

Very few engineers, when deciding whether their company can afford to design to make something as safe as it ought to be, appear to take into account (or to be allowed to take into account) the possible consequential costs to their employers of not getting functional safety right. Consequently, some companies may be exposed to much greater financial risks than they may be aware of.

5 How EM performance should be controlled to achieve functional safety

These guidelines recommend a general procedure which involves asking the following questions:

- What EM threats could the new apparatus be exposed to?
- What could happen as a result of these EM threats?
- Could EM disturbances emitted *by* the new apparatus itself affect other apparatus?
- What are the reasonably foreseeable functional safety implications of the above?
- What actions are needed to achieve the required level of safety?
- What documentation is required to show due diligence in achieving safety?

We'll now look at these six steps in a little more detail.

5.1 What EM threats could the new apparatus be exposed to?

This means discovering what EM disturbances, *however infrequent*, the new apparatus could be exposed to during its life. It requires an assessment of *all possible* EM disturbances in its intended operational environment. This is not too difficult to do with the guidance of the IEC 61000-2 series (particularly IEC 61000-2-5 and –6) and lightning protection standards such as IEC 61024-1 or BS 6651 Annex C. Where actual potential threats to the new apparatus are discovered or suspected, more detailed investigations, calculations, or instrumented surveys may be required to quantify them with greater precision.

An example of an increasingly common EM performance problem is proximity to mobile radio transmitters, such as walkie-talkies and cellphones. Although the transmitters are not *very* powerful (usually between 0.5 and 5 watts), they can be very near to an apparatus or its cables and so expose it to RF fields which are much higher than those used by harmonised immunity standards.

Foreseeable future changes to the EM environment should also be considered, such as whether the operator of the new apparatus might start using a private mobile radio system, or change his existing one to use a different frequency.

5.2 What could happen as a result of these EM threats?

Answering this means determining what are the *reasonably foreseeable* functional effects of the above EM disturbances on the new apparatus. This is required for each of the EM disturbances assessed as being significant, for each of the safety-related functions. A matrix of EM disturbances versus functions is usually the result.

5.3 Could EM disturbances emitted by the new apparatus itself affect other apparatus?

EMCD harmonised emissions standards warn that they do not cover situations *"where sensitive apparatus is used in proximity"*, but they don't specify what they mean by the words "sensitive" or "proximity". Most of these standards are also limited to frequencies below 1GHz, but modern computers can easily have significant emissions at >2GHz, and EN 55011 allows *unlimited levels of emissions* at 'ISM frequencies' for apparatus that uses radio-frequency energy to process materials.

Interference with analogue telephones, radio communication systems, and the measurement and control of physical parameters (temperature, pressure, flow, heartbeat, etc.) can easily occur. Many design engineers and system integrators still do not appear to realise that it is very easy for DC or low-frequency analogue electronics to be seriously upset by disturbances in the 100's of MHz.

It is important to also take into account foreseeable future developments in the vicinity of the new apparatus, such as the possibility that sensitive instrumentation may be installed nearby.

5.4 What are the reasonably foreseeable functional safety implications?

Answering this means assessing the reasonably foreseeable functional safety implications of the EM threats and weaknesses revealed by the previous three steps. This step should cover:

- The severity of the possible safety hazards.
- The magnitude of the risk for each hazard.
- The type and number of people who could suffer.

The safety integrity level (SIL) concept as specified by IEC 61508 can be a useful aid here.

Remember that exposure to EM disturbances (and the responses of apparatus) have statistical probabilities which should be allowed for. This usually means applying suitable 'margins' which depend upon the magnitude of the possible safety consequences.

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

The required level of safety is "*the safety that people have the right to expect*".

EM performance 'proof' testing is an obvious choice here, but if apparatus is poorly designed from an EMC point of view the test results for one unit may be meaningless for the EM performance of subsequently manufactured units of the same type. Also, actual EM performance when in use could be fatally compromised by poor EMC practices in installation, commissioning, operation, maintenance, repair, upgrading, and refurbishment.

So: actions are needed which ensure that the necessary EM performance is determined, designed-in, and tested for all critical stages in the lifecycle of the new apparatus, right from the start.

5.6 What documentation is required to show due diligence in achieving safety?

The law assumes that if it isn't written down, it didn't happen. So the project records should show that all the necessary activities were carried out from the start of a project, and that the required EM performance has been verified.

The EU's Low Voltage and Machinery Directives require documented safety arguments, so these should include any EM performance-related functional safety issues. Such documented arguments will also be valuable in reducing liability exposure.

Larger projects that require safety approvals or certification (e.g. from the HSE in the UK) should include EM performance in their safety argument (sometimes called a Safety Case). The 'Safety Argument' or 'Safety Case' approach to EM performance-related functional safety is recommended. For some projects this may be quite a slender document. An important section of these IEE guidelines is devoted to describing how such documentation can be created without imposing an unnecessary burden on the manufacturer.

5.7 Installation and maintenance instructions, limitations to use, and warnings

EM performance documentation supplied to the user should include information on each of these four issues. 'Limitations to use' can include such things as banning mobile phones from a specified area around the apparatus. Installation instructions can include the requirement for additional lightning protection measures. These all help avoid 'failure to warn' liability claims.

It has to be said here that it is *reasonably foreseeable* that people will not read these instructions, or will ignore or forget them. Since safety requires foreseeable misuse to be taken into account, lower risks would be achieved – for all concerned – by dealing with all foreseeable safety issues in design.

6 The structure of the IEE's guidance document

These guidelines are structured as a 'Core' section plus a (larger) 'Industry Annex' section.

6.1 The 'Core'

This starts with a one-page Executive Summary, followed by a section which describes the modern need to take account of EM performance-related functional safety. As well as the general procedure described in 5 above, it –

- Introduces EMC engineers to functional safety issues.
- Introduces safety engineers to EMC and EM performance.
- Introduces managers to controlling the increasingly important issue of EM performance-related functional safety, including the financial and liability benefits of controlling it correctly.
- Describes the need to take faults, errors, misuse, and maintenance into account.
- Describes the legal basis for taking EM performance into account in safety issues.
- Describes a variety of ways of making a safety argument.

– and it also encourages people to assess:

- Whether they have the required competency,
- Whether they need training, or expert assistance
- Whether they are following the ethical guidelines of their profession.

The Core also contains brief summaries of some safety incidents where a lack of EM performance has been *proven* to be the cause.

Due to the statistical nature of EM disturbances, and of the EM performance of electronic apparatus, it is thought likely that many incidents for which no fault could be found were in fact due to EM interference. Most EMC experts know of many ‘near misses’ which have never been made public, and of many accidents just waiting to happen.

6.2 The industry annexes

These guidelines also include a number of detailed ‘Industry Annexes’, each showing how a particular industry has addressed (or should address) the issue of EM performance-related functional safety. Each was written by experts from those industries. These annexes include, at present –

- Aerospace
- Building Services and Electricity Distribution
- Healthcare
- Marine Transport
- Offshore Oil and Gas
- Rail Transport
- Road transport
- Software
- Heavy industry

Although the annex on Software is not strictly an ‘Industry Annex’, it has been included because it will be especially important in the future as more and more critical systems are controlled by digital processors running software or firmware.

It is expected that these annexes will be modified, and additional annexes added, in the future as the field of EM performance-related functional safety becomes more established.

6.3 When will the Guidance document be published?

The final draft is complete, and is presently undergoing an approval process at the IEE.

If/when it is approved, it will probably be published on the IEE website (www.iee.org.uk) and hopefully will be made available for free download, probably using the Acrobat PDF format.

It is hoped that IEE approval and publication will occur during the summer months of 2000.