EMC-Related Functional Safety

EurIng Keith Armstrong
Cherry Clough Consultants
phone: +44 (0)1457 871 605
fax: +44 (0)1457 820 145
e-mail: keith.armstrong@cherryclough.com
Web: www.cherryclough.com

Published in “Safety Systems” (the newsletter of the Safety-Critical Systems Club), www.safety-club.co.uk, January 2001

One of the problems peculiar to all electrical and electronic technologies is Electromagnetic (EM) Interference (EMI). All electrical and electronic technologies emit EM disturbances that can interfere with the correct operation of radio-communications or other electronics. Modern technologies are in general more likely to cause such disturbances, worsening the EM environment that electronic devices are exposed to.

All electronic technologies also suffer from degraded functionality, including complete failure, when exposed to EM disturbances and modern electronic devices are in general more likely to be susceptible. The discipline of controlling emissions of – and susceptibility to – EM disturbances is known as Electromagnetic Compatibility (EMC).

Modern electronic technologies are being increasingly used everywhere (e.g. computers, PLCs, variable-speed motor drives, cellphones), including a very rapid increase in their use in safety-related applications. Consequently, it is becoming increasingly likely that errors in, and misoperation of, electronic devices due to inadequate EMC will cause an increase in accidents.

Many people think that all that is necessary for good EMC is for equipment and systems to meet the EMC Directive and be CE marked. Unfortunately, neither the EMC Directive nor its harmonised EMC standards

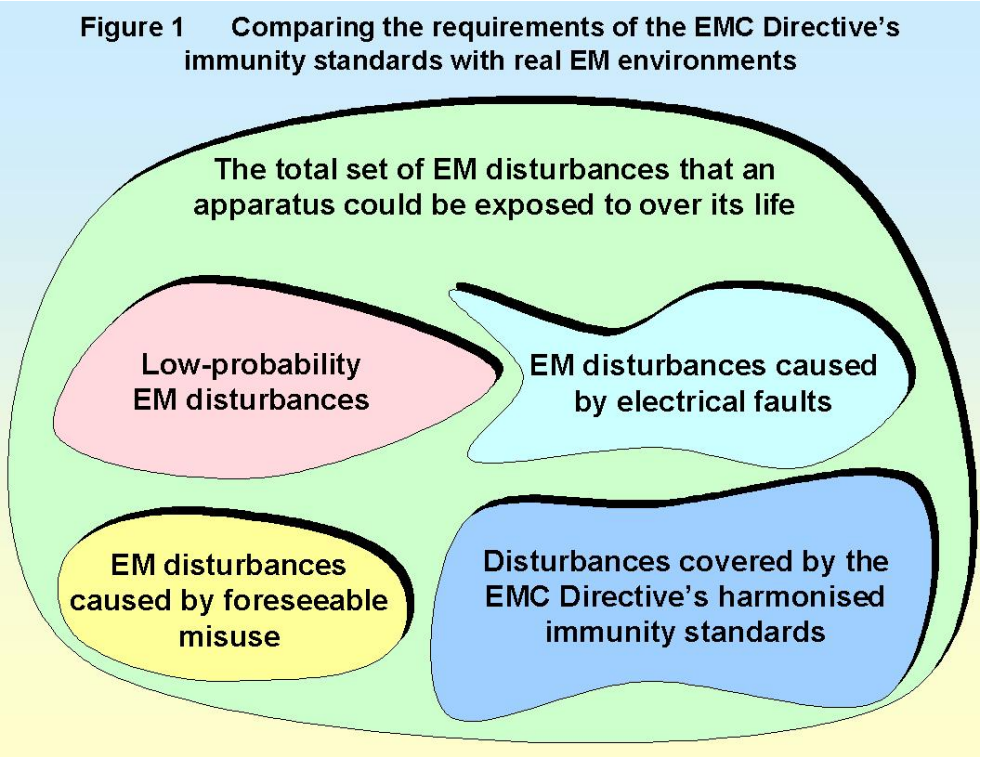


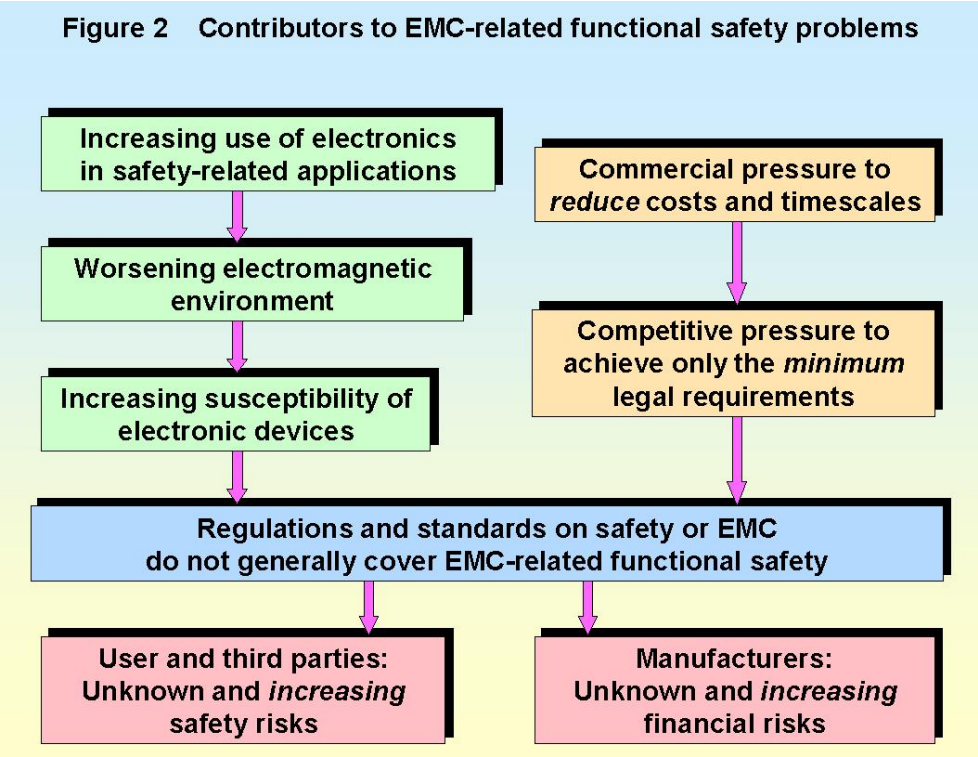
Figure 1 Comparing the requirements of the EMC Directive's immunity standards with real EM environments

cover EMC-related functional safety, as has been recognised by the European Commission. Figure 1 shows the nature of this problem.

Unfortunately, most of the safety standards which are harmonised under the Low Voltage Directive also do not cover EMC-related functional safety, and some don't even cover functional safety. The Machinery Safety Directive and its harmonised safety standards attempt to cover the EMC issues for machine safety, but eventually fail by referencing the EMC Directive and its standards – which don't cover safety issues.

Because of the lack of coverage of this increasingly important issue by existing EMC or safety standards – and also because most EMC engineers are not used to thinking in safety terms and most safety engineers

don't understand EMC – issues of EMC-related safety are 'falling between two stools'. Since the commercial pressures on manufacturers are such that they are unwilling to go further than their minimum legal



obligations, the resulting safety risks are uncontrolled, as shown by Figure 2.

Two new IEC standards and technical reports [1] [2] have begun to address these issues, but they are not yet widely understood or used. They are also not harmonised under any EU Directives and unlikely to be so for many years yet.

It may not be commonly realised that where EMI can lead to safety risks (as is increasingly likely) the EMC performance required of electrical and electronic apparatus comes under a number of EU Directives and UK laws on safety, even where they do not specifically mention EMC or EMI.
These include:
- Machinery, Low Voltage Equipment, and Personal Protective Equipment Directives
- Product Liability and General Product Safety Directives
- Provision and Use of Work Equipment, and other Health and Safety at Work Directives
- 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)

As an example of an increasingly common EM disturbance, consider the possible proximity of mobile radiocommunications to a safety-related electronic system. The EMC Directive's immunity standards require normal functional performance to be maintained when exposed to radio-frequency (RF) fields at either 3 Volts/metre for residential, commercial, and light industrial environments; or 10 Volts/metre for normal industrial environments. But what do these V/m levels mean in real life for the proximity of mobile radiocommunications?

Cellphones in poor reception areas (2W RF power):	3V/m:	2.5 - 5m
	10V/m:	0.8 - 1.6m
Typical factory walkie-talkies (4W RF power):	3V/m:	3.5 - 7m
	10V/m:	1.3 - 2.3m
Emergency services walkie-talkies (10W RF power):	3V/m:	5 - 10 m
	10V/m:	1.6 - 3.3m
Taxi or emergency services vehicle (100W RF power):	3V/m:	18 - 36m
	10V/m:	6 - 12m

The range given for the distances above is an attempt to cover possible reflections of the radio transmissions from metal objects. *Please don't use these distances as more than a very rough guide.* Where a safety-critical system is concerned the maximum distances above will need to be multiplied by a factor of at least two, possibly more than 4, depending on the Safety Integrity Level involved and the metal structure of the site. Notice that none of these distances are short enough to allow controls or keyboards to be operated by people who are also using mobile radiocommunication hand-helds.

What sorts of degraded functionality could be caused by exposure to RF fields (to continue the example)? Instrumentation can suffer from measurement errors of up to ± 100%, including:
- load cells and strain gauges (e.g. safe load indicators)
- controlled variables in exothermic reactions
- speed control
- control of flow, temperature, pressure, weight, mass, rate, position, etc.

Computers, PLCs, and computerised equipment can suffer from:
- false key-presses, leading to uncommanded operational mode changes (e.g. from crawl to full speed)
- false data (e.g. ignoring a limit switch)
- incorrect operation of software (e.g. continually repeating an inappropriate subroutine)
- total failure (often called a crash) which can leave control outputs in *any possible combination of states,* including those that could damage the equipment and may not have been foreseen by its designer.

To properly account for EMC issues for functional safety, hazard and risk assessments should consider the following:

a) What EM disturbances, however infrequent, might the apparatus be exposed to?
b) What are the reasonably foreseeable effects of such disturbances on the apparatus?
c) How might the EM disturbances *emitted* by the apparatus affect other apparatus (existing or planned)?
d) What could be the reasonably foreseeable safety implications of the above mentioned disturbances (e.g. what is the severity of the hazard, the scale of the risk, the safety integrity level required)?
e) What level of confidence (e.g. verification? proof?) is required that the above have been fully considered and all necessary actions taken to achieve the desired level of safety?

Such assessments, and the decisions, specifications, work activities, and verifications that arise from them should be treated as part of the safety validation and documented. In general, where hazards and risks are higher (i.e. a higher safety integrity level applies), a higher level of activity, competence and documentation is required.

An IEE Working Group consisting of experts from both EMC and Safety disciplines, including senior HSE personnel, created the IEE's professional guidance document on EMC and Functional Safety [3] [4] in mid-2000. This is intended to raise the awareness of EMC-related functional safety among directors, managers, designers, health and safety inspectors and other professionals, and to provide guidance on how best to deal with EMC-related functional safety.

The IEE Guide also provides background information on EMC, safety arguments, laws, etc., to help bridge any gaps between the EMC and safety disciplines in an organisation; and there is a section describing a number of safety incidents where the cause was officially attributed to EMI.

A number of more detailed 'Industry Annexes' to the Guide describe what some industries are already doing to control EMC-related functional safety, pointing out their shortcomings. Two of the annexes are proposals for industries which don't have established procedures (offshore oil and gas, and heavy engineering where projects are performed by subcontractors). An annex on software is also included, describing established guidelines for the design of robust software.

Many companies are not very familiar with the EU's Product Liability Directive (PLD). It might be possible to achieve a defence of due diligence when complying with CE marking directives even though issues of EMC-related safety have been ignored. But the only real defence under the PLD is the 'state of the art' or 'development risks' defence, and to be able to employ this defence successfully in the event of claim means that all relevant safety knowledge, such as [1] [2] and [3], should have been taken into account in the design.

For more details on this increasingly important safety issue, read [5] and [6].

References and further study:

[1] *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

[2] *IEC 61508* (seven parts) Functional safety of electrical/electronic/programmable electronic safety-related systems

[3] *IEE Guidance document on EMC and Functional Safety*
Institution of Electrical Engineers, London, 2000
Downloadable free from: www.iee.org.uk/Policy/Areas/Electro/ as a 'Core' document and nine 'Industry Annexes' in Word or PDF formats (Note: the URL may be case sensitive).

[4] *EMC and Functional Safety*
Keith Armstrong, IEE Review, November 2000, pp 34-37

[5] *EMC-Related Functional Safety*
Keith Armstrong, ITEM UPDATE 2001, available from www.rbitem.com

[6] *New Guidance on EMC-Related Functional Safety*
Keith Armstrong, 2001 IEEE EMC International Symposium, Montreal, August 13-17 2001 (session D3-P3, 15th August). Conference Proceedings: ISBN 0-7803-6569-0/01, pp 774-779

Websites for downloading copies of all the directives mentioned above are listed at www.cherryclough.com.