IEE Guidance Document on

EMC and Functional Safety

Table of contents

This document is organised as a main part (called the **Core**) and a number of **Annexes**.
Each Annex has its own table of contents.

1. Introduction and purpose

One of the problems peculiar to all electronic technologies is electromagnetic (EM) interference. All electrical and electronic technologies emit EM disturbances that can interfere with the correct operation of radio-communications or other electronics. Modern electronic technologies are in general more likely to cause such disturbances than those they replace.

All electronic technologies can also suffer from degraded functionality (including complete failure) when exposed to EM disturbances. Modern electronic technologies are in general more likely to be susceptible in this way than those they replace.

The discipline of controlling emissions of, and immunity to EM disturbances is known as Electromagnetic Compatibility (EMC).

Electronic technology is increasingly used in safety-related applications. Consequently, errors and misoperation of electronic devices due to inadequate EMC can result in hazardous situations with an increased risk of harm to people's health and safety.

Companies who are well versed in the safety of their traditional technologies may not be aware of the possibilities for increased risks associated with the use of electronic technologies. For example, a machinery manufacturer may use a programmable logic controller (PLC) to control a machine. When the PLC is interfered with, for example by EM disturbances from a nearby walkie-talkie, or by a voltage transient on its mains supply, it is possible that the machine could make an unintended movement – possibly putting nearby workers at increased risk of injury or even death.

The EMC and safety divisions within an organisation tend to use different skills and disciplines and may operate largely independent of each other. Important issues of EMC-related functional safety may 'fall between two stools' and not be correctly addressed.

The purpose of this report is to raise the awareness of EMC-related functional safety among directors, managers, designers, and other professionals. It will show that compliance with the EMC Directive (or its harmonised standards) may not ensure that EMC-related functional safety issues have been correctly addressed and relevant safety legislation met.

This report also provides guidance on how to deal with EMC as regards functional safety, and should help bridge any gaps between the EMC and safety disciplines in an organisation.

Which sections to read?

- Directors and everyone else should read sections 1 – 3 of the 'Core'
- Project managers, and practitioners of EMC or safety should also read Core sections 4-8
- More depth on EMC, safety, and legal issues are provided by Core sections 9 onwards
- Annexes show how EMC-related functional safety issues are being controlled (or are proposed to be controlled) in a number of different industries, and also for software

Where people responsible for EMC or safety cannot understand all of this guidance document, or cannot effectively put its recommendations into practice, they should obtain specialist assistance.

Note 1: EM disturbances can be directly hazardous to health. This document concerns functional safety – where the accuracy or reliability of electrical or electronic apparatus has implications for health and safety.

Note 2: This document is not prescriptive in any manner, but is based on the best understanding and practices at the time of writing. It does not supplant the need for professional, legal, or technical advice in specific circumstances.

2. Executive Summary

Whenever electrical or electronic technologies are used in control or protection, it is possible that risks to health and safety may be caused or increased by errors or malfunctions due to a lack of adequate electromagnetic compatibility (EMC).

To meet legal requirements for the supply of safe goods, product liability, and health and safety at work, it is necessary to correctly address the issue of EMC with regard to functional safety.

The EMC Directive does not specifically cover safety issues, so CE marking under the EMC Directive (including its harmonised standards) may not provide adequate EMC performance for functional safety.

To correctly control EMC-related functional safety, hazard and risk assessments are needed. The following should be considered:

a) What electromagnetic (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 (what is the severity of the hazard, the scale of the risk, the safety integrity level required)?

e) What level of confidence (verification? proof?) is required that the above have been fully considered and all necessary actions taken to achieve the desired level of safety?

These hazards and risks assessments, and the decisions, specifications, activities, and verifications that arise from them should be treated as part of the safety validation, and be documented.

The amount and quality of the above actions and documentation can vary significantly from one organisation to another, and from one project to another. In general, where hazards and risks are higher (i.e. a higher safety integrity levels apply), a higher level of activity and documentation is required.

The personnel responsible for managing and implementing EMC and safety in an organisation all need to understand this document, be competent to perform their activities, and must correctly put these guidelines into practice on a routine basis. If they are unsuited or unable to perform any of these, specialist assistance is required.

Note 1: The use of the word “electronic” in this report includes programmable electronic apparatus.

Note 2: This document is not prescriptive in any manner, but is based on best understanding and practices at the time of writing. It does not supplant the need for professional, legal, or technical advice in specific circumstances.

3. The need to consider EMC to achieve functional safety

This report is concerned with the relationship between EMC and functional safety, and is intended to act as an overview of the relevant engineering and legal liability aspects in plain English for all practising engineers of whatever discipline, and their managers and directors. Issues of health and safety at work, consumer, third-party, and public safety are all addressed.

There is a proliferation of electronic controls in almost every aspect of human life, especially caused by the rapid progress in digital processing that allows "intelligence" to be added to even the lowest-cost products. Whilst electronic controls and "intelligence" add increased functionality and bring many other benefits, they also suffer from performance and reliability problems which are peculiar to the various electronic technologies they use.

One of the problems peculiar to *all* electronic technologies is EM interference. All electronic technologies emit EM disturbances that may interfere with the correct operation of radio-communications and other electronics. All electronic technologies can suffer from degraded functionality (including complete failure) when exposed to EM disturbances in their working environment. The control of emissions of, and immunity to, EM disturbances in all electrical and electronic apparatus is known as EMC.

Different electronic technologies have differing potential for suffering functional performance degradations when exposed to EM disturbances. Many of the long-established electronic technologies, which did not suffer unduly from EM interference when first introduced, are now suffering from increased levels of interference due to increases in the EM disturbances in their operating environments. Newer electronic devices (silicon chips) tend to be more susceptible to EM disturbance than the devices they replace.

EM interference to electronic technologies can result in an increased exposure of people to existing safety hazards, and can also result in new types of safety hazards. Companies who are well versed in the safety issues relevant to their traditional fields may find themselves unaware of the possibilities for increased or new safety risks caused by the use of new electronic technologies, or may lack the necessary skills to deal with them effectively.

3.1 EMC and Safety-Related Systems

A system is classified as ‘safety-related’ if some property of the system in some way affects safety [1]. The term is usually used to describe those systems which are required to perform a specific function or functions to reduce risks to a level which is considered to be tolerable [2]. Safety-related systems may be implemented in any technology, but in the context of EMC, interest is in those systems which are implemented in electrical or electronic (including programmable electronic) technologies.

For example, the following are examples of electrical / electronic safety-related systems:

- an emergency shut-down system in a hazardous chemical process plant
- a crane safe-load indicator
- a railway signalling system
- machinery guard interlocking and emergency stop arrangements
- a variable speed motor drive used to control ‘crawl speed’ as a means of protection
- the system for interlocking and controlling the exposure of a medical radiotherapy machine
- the air bags, anti-lock braking, and engine-management systems of a motor car.

3.1.1 Safety integrity

Key to the understanding of safety-related systems is the concept that a safety-related system carries out safety functions; and that a safety function should be specified both in terms of functionality (what the function does) and safety integrity (the probability of a safety function being performed satisfactorily when it is required).

The specification for safety integrity is derived by undertaking a hazard & risk analysis and determining the extent of risk reduction which the particular safety function brings about [1]. The general principle is that more rigour is required in the engineering of safety-related systems at higher levels of safety integrity in order to achieve the lower failure rates which are required to achieve tolerable risk.

3.1.2 Safety requirements

The safety requirements for electrical or electronic equipment used in safety-related systems should be well specified and derived in the context of a system hazard and risk assessment during an early phase in its safety lifecycle [3]. The immunity aspect of EMC is an important safety requirement which should be addressed at this stage. This involves the following stages:

a) The EM environment which will be encountered during operation of the equipment should be specified in terms of types of disturbances and their characteristics, for example levels, frequencies or extent. Due to statistical variations it will not be possible to specify absolute levels which will never be exceeded. The aim should be to specify limits which will only be exceeded with a defined probability, for example 5%, appropriate to the safety integrity level required.

   If it is necessary to impose any special controls on the use of other equipment (e.g. cellphones and other mobile radiocommunications) in order to allow higher confidence that limits will not be exceeded, then such controls should be specified at this stage. But controls which rely on people doing as they are told are often flouted, and the required safety integrity level may be so high that even occasional lapses may not be acceptable.

   Standards may assist in this process [4] but should not be relied on totally. Knowledge of particular environments is important and should not be neglected. Standards may have neglected certain types of disturbance which may be important in a particular EM environment. Also, the EM environment itself is always subject to change due, for example, to changes in frequency allocations, the introduction of new equipment, and modifications to existing products, systems, and installations. In particular it should be recognised that standards harmonised under the EMC Directive [5] should not be used, without other considerations, as a basis for specifying safety requirements (section 10 has more on this).

b) The EMC immunity limits for the equipment should then be derived taking into account both the EM environment and the required safety integrity of the safety functions involved. The immunity limits are the minimum levels of disturbances which the equipment should withstand without its operation being interfered with (or degraded) in a way which could lead to danger. The difference between the specified limits of the environment (assessed disturbance levels) and the immunity limits is, in effect, a safety margin (sometimes called a compatibility margin [6]).

   This margin should be derived taking into account both the statistical nature of the environment and the required safety integrity of the safety functions. In principle, a higher safety margin is required where there is uncertainty about the environment and / or when the equipment is intended to perform safety functions at higher levels of safety integrity.

   This will probably be a mainly judgmental process. It will probably not be practical to fully quantify, for example, the statistical distribution of the EM environment. A key point is that

the requirements should be consciously and openly determined in the full knowledge of the system safety requirements and by personnel with relevant EMC expertise having experience of the intended environment and application (see section 14 for more on competency).

c) The test procedures and performance criteria which will be used to validate the immunity levels should then be specified. Performance criteria for immunity testing should take into account the hazards and risks associated with the application. For example, even temporary degradation of performance or loss of function may not be acceptable in some applications.

d) Even during servicing and maintenance procedures, safety is still required, so maintenance and modification procedures should consider EMC. In particular, the use of mobile radiocommunications close to equipment which has had covers removed should be carefully controlled, particularly when equipment is being maintained 'on-line'.

e) Software changes and upgrades can also negatively affect EMC and hence functional safety, so these should be treated as for hardware maintenance.

f) The above has dealt with the immunity of a product, system, or installation to its EM environment, but it must not be overlooked that some equipment can emit EM disturbances which can markedly worsen their local EM environment, possibly causing degraded functionality in other equipment. Audio or radio communication systems can be very susceptible to EM disturbances, which can lead to safety risks if they are used to communicate safety information. Some industrial, scientific, or medical equipment utilises radio frequency (RF) energy at high powers to perform its intended function (e.g. induction heating, plastic RF welding or sealing, RF-assisted metal welding), and emissions from these can cause errors in nearby instrumentation or control, with possible safety risks.

So, when planning new equipment, steps need to be taken to ensure that its EM disturbances do not reduce the compatibility margins for the existing equipment below what is necessary for its functional safety.

3.1.3 General points

- EMC testing is unlikely to reveal all the potential modes of functional degradation which may result from EM disturbances. In this respect, the achievement of EMC in the context of safety should be approached in a similar way to that necessary for safety-related software. That is, it is important that a systematic approach is adopted at all stages of the safety-lifecycle [8] in order to avoid, as far as possible, the introduction of systematic faults.

  It is particularly important that EMC is considered at an early stage during the design of equipment as it is often then that the most effective measures can be taken (this is also likely to be the most cost-effective way to ensure EMC).

- In some applications it may be acceptable, for safety, for an EM disturbance to cause the equipment to fail, but in a way which ensures a safe state. For example, it would be preferable for a light curtain on a paper cutting guillotine to cause a lock-out of the machine, rather than continue to operate with reduced detection capability as a result of mains supply voltage dips.

- EM disturbances may be the cause of "common-cause faults". These are identical faults which occur at the same time in different parts of a system due to a common cause. It is particularly important to consider these in safety-related systems which employ redundant architectures as a means of protecting against random failures of hardware components. Estimates of hardware reliability should take into account the possibility of such common-cause faults [7] because they can significantly increase the likelihood of failure from that which results from consideration of random failures only.

- Where protective devices (e.g. varistor transient suppressers) are used to achieve a level of immunity and where failure of such a device could cause a reduction in immunity level which

could lead to danger, then the failure of such devices should either be detected automatically (for example by the action of diagnostic tests) or the devices should be tested on a regular basis to reveal any failures. The periodicity of such tests would need to be determined on the basis of the acceptable probability of failure in a particular application.

- It is vital that the designer makes sufficient information available to, and that such information is used by, the manufacturer, installer, operator and maintainer to ensure that the intended EMC protection measures are implemented and maintained to preserve the intended levels of emissions of, and immunity to, EM disturbances.

- Assessing EMC-related functional safety risks is a difficult field with little published guidance. Personnel involved in EMC-related functional safety activities require specific skills and knowledge that may not be shared by practitioners of EMC or safety alone (see section 14 for more on competency).

4. Guidelines on controlling EMC to achieve functional safety

To control EMC correctly for functional safety reasons, hazard and risk assessments must take EM environment, emissions, and immunity into account. The following should be addressed:

- the EM disturbances, however infrequent, to which the apparatus might be exposed;
- the foreseeable effects of such disturbances on the apparatus;
- how EM disturbances emitted by the apparatus might affect other apparatus (existing or planned)?
- the foreseeable safety implications of the above mentioned disturbances (what is the severity of the hazard, the scale of the risk, and the appropriate safety integrity level?); and
- the level of confidence required to verify that the above have been fully considered and all necessary actions taken to achieve the desired level of safety.

4.1 A general procedure for controlling safety risks due to EMC

The following is a brief outline of a procedure which should ensure that safety-related hazards and risks due to EMC issues identified in 3.1.2 are properly addressed, whether for a product, system, or installation, collectively known as apparatus.

a) **EM Environment.** Qualify and quantify the exposure of the apparatus to the EM disturbances present in its intended operational environment(s), taking into account likely (or possible) changes to the environment(s) in the future. This should include all reasonably foreseeable exposure to EM disturbances *of whatever kind.*

   Also qualify and quantify the EM disturbances emitted by the apparatus, and their reasonably foreseeable effects on other apparatus which may have safety implications if interfered with.

   IEC 61000-2-5 [4] will be found helpful for guidance on assessing EM environments, and the kinds of disturbances emitted by some apparatus (bearing in mind that it was not written for safety purposes and only focuses on “typical” environments). Annex J includes a table of EM disturbances which may also be useful.

b) **EM Specification.** Determine the acceptable immunity and emissions performance criteria for each safety-related function of the apparatus, for each of the EM disturbances identified above, to achieve the desired ‘compatibility margins’ for the appropriate safety integrity levels.

   The results are often most conveniently expressed as a table (matrix) of function versus EM phenomenon, with the performance criteria in the cells. (This is a hazards and risks assessment, and may result in different functional performance criteria than are required for compliance with the EMC Directive).

c) **Design, build, verify, maintain.** Ensure that all necessary steps are taken throughout the apparatus’ entire life-cycle (including maintenance, upgrade, or refurbishment) to meet the EM functional performance criteria specified above, and that appropriate validation occurs before supply and after maintenance, modification, upgrade, and refurbishment.

   Validation should ensure that the product's required functional performance is actually achieved in its intended operational environment(s), and that its safety is as required by the relevant laws and the reasonable expectations of its users and other affected persons. Some customers or users may have their own requirements for validation.

d) Inform **and warn.** Inform prospective and actual purchasers and users of the apparatus' intended EM environment, any limitations to use, operator skill and/or training requirements, and possible performance degradations. Also warn of any potential risks from unusual or high energy emissions. For engineering projects: include these warnings, limitations, requirements, and specifications in all tender documents and contracts.

   Warning of a safety hazard is considered no substitute for guarding against it – where guarding is possible. Guarding is considered no substitute for designing the hazard out in the first place – where it is possible to design the hazard out.

e) **User Instructions.** Provide all the installation, use, and maintenance instructions necessary to define the EM environment that the apparatus is intended for, and achieve and maintain the required EM performance.

   It is also recommended that a description of how EM interference may appear to the user, and the simple mitigation measures that the user can take, be included. IEC 61000-5-2 and IEC 61000-5-6 are recommended for guidance on good EMC build and installation practices.

f) Marketing **and Sales.** Ensure that marketing and sales people advertise and sell only to the intended EM environment(s), and that they don't 'gloss over' or fail to communicate any limitations to use, skill requirements, degraded performances, or special installation and use requirements.

   This is often very difficult to achieve in practice, but should not be ignored because an inappropriate sale can negate all the care that has been taken in design and validation, and expose a company to legal penalties even though no safety incident has occurred.

4.2 Procedures, documentation, and evidence

Some organisations control the EMC of new projects or apparatus with an EMC Control Plan, to make sure that cost- and time-effectiveness is optimised whilst meeting all EMC requirements. An "EMC and Functional Safety Control Plan" could likewise be used to ensure that the measures briefly described above are fully implemented in the most cost-effective manner.

Whatever title this activity is given, documentation should result. Documentation should provide instructions and procedures, record activities and clear statements of outcomes. If an action is not properly documented it can be very hard to prove in a court of law that it took place. This can be a serious problem for any organisation subjected to a safety audit or investigation.

Safety planning, procedures, and documentation should start from the beginning of any new project to help achieve the required levels of hazards and risks without wasting time or money.

Small organisations whose activities cannot create safety problems (perhaps because their activities create small hazards, or not many people are exposed) usually spend less time/money on documentation than big organisations. But whatever the size of an organisation – if high levels of safety hazards/risks are created, significant time and cost should be spent on safety procedures and documentation.

Even the smallest organisation (such as a one-man company) should carefully decide what sorts of arguments they should use, and evidence they should marshal, to demonstrate that their activities produce safety hazards and risks that are no greater than the law requires and people have a right to expect. Anything reasonable could be used to make a convincing safety argument.

It is well to remember that the law's requirements and people's expectations change with time, and what was acceptable a year ago (or before a publicised safety incident) may no longer be acceptable.

Section 12 (‘Making a case for safety’) expands on this theme, to provide the basics of a “safety case” approach which may be used by a very wide range of organisations, from the smallest to the largest.

Section 13 gives a brief outline of the “Safety Case” approach which has been developed by a number of safety-critical industries jointly with the HSE over many years. This tends to be used in large engineering projects (e.g. rail networks) and is included here for information only. Many other alternatives to the Safety Case approach have been developed over the years in different industries, and have been described in a number of publications.

An organisation’s activities may be covered by one or more EU Directives, national laws, or industry codes of practice, and these may mandate certain safety activities, procedures, or documentation (refer to the section on Legal Liabilities). But almost all the Directives, laws, and codes created so far make no mention (or very little) of the safety issues which may be caused by inadequate control of EMC. This is one of the reasons for this report. So, when following any safety procedures or creating any safety documentation in future, it is most strongly recommended that the EMC and functional safety issues raised by this report are taken fully into account.

5. Faults, errors or misuse, and maintenance

EMC legislation requires apparatus to exhibit a degree of immunity by complying with certain performance criteria. These criteria may be not be acceptable under safety legislation. Under safety legislation apparatus is required to be safe even during reasonably foreseeable faults, error or misuse, and also during maintenance. So where an EM disturbance could give rise to safety hazards or risks during faults, maintenance, errors or misuse, this is covered by the safety legislation.

5.1 Fault conditions

Fault conditions can give rise to excessive emissions of EM disturbances, e.g. when a fuse opens it can cause a voltage surge of up to double the AC supply voltage – which could prove too much for neighbouring equipment. Fault conditions can also cause the immunity of an apparatus to be compromised, e.g. when an earthing strap comes loose, or a cable shield is damaged.

It is recommended that (as for the removal of panels during maintenance, see 5.3) the designer of the apparatus must take account of reasonably foreseeable fault conditions and, given the intended use of his apparatus, make sure that appropriate measures are in place to prevent safety risks from being increased significantly. The techniques of 'fail-safe-design' should be used as appropriate.

The hazards and risks analysis for an apparatus, always recommended as a tool for helping to achieve a safe apparatus, should always include reasonably foreseeable faults.

5.2 Errors or misuse

Reasonably foreseeable errors or misuse also need to be considered in any comprehensive hazards and risk analysis. One example is where incorrect installation (a common problem) could increase safety risks and/or hazards. Another possibility is incorrect application; for example the use of an ordinary domestic or industrial electronic device in a life-critical medical application.

It is often possible to design so that errors and misuse do not result in unsafe situations, providing all the reasonably foreseeable errors and misuse have been identified early in a project's design cycle. This is always the preferred way to deal with such issues. Where problems cannot be designed out, it may be acceptable to guard against them in some way. Where design and guarding are not totally adequate, it may be acceptable to deal with the potential for errors or misuse by careful marking of the product, by warnings in the user manual, by making sure that marketing and sales efforts do not give the wrong impression, and by making sure that salespeople are trained appropriately.

Where significant safety hazards or risks exist, it may be necessary to deal with the issue of possible errors or misuse by *insisting* that the apparatus is installed and/or commissioned by competent personnel who have the appropriate training, or that the work of the installers/commissioners is checked by someone with the necessary competence and specific knowledge. These could be the employees of the apparatus manufacturer himself. Such control of competency during installation and commissioning is already accepted practice in the high-voltage power industry because the (financial as well as safety) consequences of making a mistake are too high to contemplate. It may even be necessary to refuse to supply safety-related apparatus unless such contract terms are accepted by the user, and implemented in full. For such systems and installations, similar requirements will need to be in place to cover any modifications, upgrades, or repairs

5.3 Maintenance conditions

Whilst most managers and maintenance engineers are aware of the need for basic electrical safety and precautions against electrostatic discharges, their awareness of other EMC phenomena is often minimal. During maintenance work emissions of EM disturbances can substantially increase, and immunity to the EM environment can reduce considerably. The impact of this will vary on the precise situation, but an awareness of some of the fundamental issues is important.

It should be noted that the owner of the apparatus has a legal obligation to ensure that it does not create radio interference, and that it continues to comply with the safety legislation, at all times during its working life.

Doors and covers (such as inspection panels, gland plates, inspection accesses) often provide a dual function of safety and EMC protection. Consequently managers and maintenance engineers need to be made aware of the potential impact of opening doors, and removing covers, shielding, earthing wires, etc. from equipment during maintenance.

The resultant increase in radiation may affect radio reception over long distances, particularly where the equipment is high in a building; e.g. lift motors. Effects may range from annoyance, to the blocking of safety and distress services. At a local level, care should be taken to avoid the effects of blocking telemetry and control receivers. It is recommended the designer of the apparatus takes service and maintenance requirements into account, given the intended use of his apparatus, to make sure that appropriate measures are in place (or are taken by those performing the maintenance, given their level of competence) to prevent safety risks from being increased significantly. The hazards and risks analysis for an apparatus should always include considerations of servicing and maintenance.

Similarly the immunity of equipment can be impaired during maintenance. Engineers carrying mobile phones whilst working on the equipment may cause it to be over stressed and suffer functional errors or damage. The impact of this is not easily predictable. It is recommended that managers should assess their safety procedures with respect to their policies on the use of radio equipment during maintenance operations. Note that cellphones transmit regularly (at full power) when switched on and in standby mode.

Whilst the mechanical and electrical safety requirements may be adequately met by the partial refitting of covers, such poor quality re-assembly will usually have an adverse impact on the EMC performance of the apparatus. It is therefore important that covers, shielding, etc. be correctly refitted after any maintenance work has been completed. Items such as spring clips, gaskets and screws play a key part in this, and all should be replaced in the manner in which they were originally assembled, with any damaged or broken parts renewed. The correct types and assembly of cables and connectors are also vital for achieving EMC performance, and any cables or connectors that are damaged or removed must be replaced using exactly the same types as originally fitted, assembled in exactly the same way. It can also be important in some installations for cables to follow exactly the same routes as when they were originally fitted.

Appropriate warning signs may be required where it proves impossible to completely design out a particular EMC-related safety risk, but these are not always suitable because it is known that people do not always read signs, or follow them when read. In certain safety-related systems the hazards are too great to permit the risk involved in assuming that someone will always take heed of a warning sign, especially when they are under time pressure.

6. The economic arguments for following these guidelines

The economic case for following these guidelines is simply that the 'cost of failure' will far exceed those associated with implementing good EMC design practices required to avoid failure. "Failure" in this context meaning a safety incident caused by the interaction of an EM disturbance and the apparatus.

It is not possible to quantify the actual 'cost of failure', however the following consequential penalties should be considered:-.

- Liabilities following on from the failing event, personal injury, property damage, loss of revenue, loss of services etc.
- Product recall
- Product forfeiture
- Product withdrawal
- Adverse publicity and its impact on future sales

The 'costs of failure' will vary from product to product, e.g. those associated with an safety failing in a high volume consumer product such as an automobile will generally be significantly higher than those for a bespoke control system for an industrial plant.

The 'costs of failure' should be compared to those of incorporating mitigation measures during the design cycle of the product, plus the cost of a realistic EMC and functional safety test programme.

Foreseeable operational EM environment(s) need to be assessed, including low-probability disturbances and electrical faults, and suitable EMC mitigation measures included at the design stage. These would include:

- Appropriate systems design and electronic architecture
- Incorporation of filters, transient suppression components, etc.
- Enclosure screening effectiveness
- PCB design and layout
- Types of interconnecting cabling and connectors and how they are assembled
- Software resilience

These costs are minimal when compared to the potential costs of an safety incident.

7. Examples of EMC-related safety incidents

The following examples illustrate some of the ways in which inadequate EMC may create hazardous situations.

A significant number of EMC-related malfunctions are known to occur, as may be seen from the regular items on this issue in Compliance Engineering Magazine (USA) and the EMC Journal (UK), among other EMC or Safety industry publications. A great many more incidents or potential incidents are known to employees and consultants working in these industries, but they are bound by confidentiality agreements and so these do not get reported. It is suggested that the actual rate of EMC-related malfunctions exceeds those reported in the press by several hundred or even several thousand-fold, and an increasing number of these will have safety implications as electronic technologies become more widely used in safety-related systems.

However, the following examples are based on safety incidents which have been officially investigated (usually by the HSE) where lack of EMC has been shown to have been an important contributor. These examples should not be regarded as definitive reports.

7.1 Radiation monitor de-activated by mobile phone

A safety monitor used to detect radiation (alpha particles) in a laboratory was switched off when a nearby mobile telephone was used. The monitor was connected to the electrical supply via a portable residual current device (RCD) BS 7071:1989. This device was tripped by the radio frequency signal transmitted by the telephone which was about 1.2m away. There was no warning that the monitor had switched off leading to a potential hazard from undetected radiation.

Ref: The Radiation Protection Adviser, 1997.

Conclusions: It is not appropriate to allow the unlimited use of mobile telephones in the vicinity of RCDs which are used to protect essential services. The provision of RCDs on the electrical supplies to safety and on-line monitoring equipment should be carefully considered and all the risks assessed. Means by which staff could be alerted to the loss of power to the safety monitors (such as an alarm), or fail-safe design techniques, should have been implemented.

7.2 Failure of safety interlock on an electrical test instrument

The high voltage output of an electrical test instrument was designed to switch off under the control of a switch fitted to the door of a test enclosure. This was intended to allow an operator of the test rig to change the item under test safely. During testing of cable-loom assemblies the operator received an electric shock. It was found that electrostatic discharges (ESD) applied to the case of the tester could cause the high voltage output to be turned on even though the interlock switch was in the 'safe' position. The test instrument also reacted in a number of different ways to the application of mains-borne interference. In this case, the high voltage output was under the control of a microcontroller.

Conclusions: The immunity of the test instrument to ESD and mains transients was not adequate leading to the possibility of serious electric shock. Safety interlocking functions should only be carried out by circuits of proven integrity. Safety interlocking functions should not be entrusted to microcontrollers, microprocessors, etc. unless the safety integrity of such control circuits has been formally validated as being adequate in relation to the risks associated with the application.

7.3 Roof support in coal mine lowered inadvertently

An incident occurred at a coal mine on a set of hydraulically powered coal face roof supports (commonly known as "walking chocks"). The roof supports were arranged so that they were controlled by a central processor in the main roadway to the coal face. They were connected in batches of 10 supports along a 200 metre longwall advancing coal face. Each support had its own microprocessor communicating with the central processor. Each batch of ten supports lowered (in turn) from the roof and then moved forward after the coal cutter had passed by removing a 1 metre strip of coal from the coal face. The sequence of events was initiated by an infra-red transmitter mounted on the coal cutter.

One of the supports apparently lowered without anyone touching it and without a command being sent from the central processor. The subsequent investigation found that mains-borne interference had generated the correct address code for the roof support processor and also resulted in the instruction to ‘lower’ being issued. The problem was solved by putting filters on the mains supply and by requiring the data message to be repeated before the roof support responded to the request.

Conclusions: Immunity to EM disturbances can be achieved by both hardware and software means.

7.4 Gas detector disabled by VHF radio

A microprocessor-based portable gas detector used by a water utility company in a sewer switched itself off when a VHF ‘walkie-talkie’ was operated nearby. The detector was being used to warn people involved with sewer repair work of the presence of toxic gases.

Conclusions: Fail-safe design should have been implemented on the gas detector. Those who use, or install, electronic instruments in safety-related applications should be aware that the operation of such instruments can be affected (possibly dangerously) by hand-held radios and telephones even though the radios or telephones may conform to the relevant standards.

7.5 CNC controlled machine affected by arc welding

The operation of a computer numerically controlled (CNC) machine was affected by a nearby arc welder which used radio frequency energy to excite the arc. It was found that the welder was earthed by connection to a stanchion which acted as an antenna. Direct grounding of the RF welder through the concrete floor solved the problem.

Conclusions: Attention should be paid to the electrical installation, particularly earthing, of equipment which uses RF energy (such as welders, heaters, sealers, etc.) to prevent interference with nearby equipment which could lead to people being injured. Manufacturers’ instructions should be followed.

7.6 FDA asks for increased wheelchair EM immunity

Tests by the US Food and Drug Administration’s Centre for Devices and Radiological Health have shown that some types of electric wheelchairs are susceptible to RF fields of 5 to 15V/m. At the lower end of the susceptibility range the brakes release, which could result in rolling if the chair happened to be stopped on an incline. At higher intensities some wheelchairs moved of their own volition even on a flat surface. CDRH has asked wheelchair makers to include EMC data in pre-market notification submissions, and has been working with them to raise the immunity of new products to 50 V/m. The FDA’s initiative was triggered by reports of erratic, unintentional powered wheelchair movement, some of which resulted in injury.

Ref: Compliance Engineering Fall 1995 p 27.

Conclusions: The immunity standards harmonised under the EMC Directive and intended to apply to the domestic, commercial, and light industrial environments apply RF field tests only up to 3 V/m, and those for the heavy industrial environment go up to 10 V/m. However, the above example shows that real environments can contain RF fields significantly greater than these levels. So it is clear that meeting EMC Directive standards may not be adequate for safety-related equipment.

7.7 Aeroplanes and laptops

A routine flight over Dallas-Fort Worth was disrupted when one of the compasses suddenly shifted 10 degrees to the right. The pilot asked if any passenger was operating an electronic device, and finding that a laptop computer had just been turned on requested that it be turned off, whereupon the compass returned to normal. Following RTCA guidelines the pilot requested that the laptop be turned on again 10 minutes later, when the compass error returned.

Ref: Compliance Engineering (European edition) Nov/Dec 1996 p12

Conclusions: Personal electronic devices can interfere with some aircraft navigation systems. It is often possible to verify that problems are caused by EM interference problems, and find their sources, if appropriate steps are taken at the time the interference occurs.

7.8 Automatic safe load indicator

An automatic safe load indicator (ASLI) fitted to a crane on board ship suffered a permanent change in its calibration ROM when the radio operator strung an extension to his aerial onto the crane jib to increase the transmitter range whilst at sea.

Conclusions: Safety-critical items should always be designed to fail-safe when subjected to extreme interference.

7.9 Fire detectors on offshore platform activated by hand-held radio

Transmitted RF signals from UHF hand-held radios caused the spurious operation of fire detectors on an offshore oil installation. It was found that the grounding and screening of the detectors was inadequate in part because of the practice of grounding cable screens at one end only.

This is common practice for electrical installations in potentially explosive atmospheres.

Conclusions: Spurious operation of protection systems can result from inadequate immunity. This can have an impact on safety because the availability of the protection system may be reduced. Careful attention should be paid to the grounding and screening arrangements for safety-related systems operating in potentially explosive atmospheres to preserve both adequate EMC and explosion proof properties.

7.10 Voltage spikes damage PLC power supplies on offshore drilling rig

Voltage spikes caused damage to programmable logic controller (PLC) power supplies and led to loss of control to variable speed drives on an offshore drilling rig. The spikes were due to very high loads supplied by SCRs with inadequate filtering. The damaged components were varistors which were intended to prevent voltage spikes being conducted into the electronics.

Conclusions: Components used to protect against EM disturbances should be rated adequately taking into account the reasonably foreseeable EM disturbances in their intended environment. Equipment should not be sold into EM environments they have not been characterised for.

7.11 Failure of a valve controller released chlorine gas

A microprocessor-based valve control panel used to control the flows of chlorine and nitrogen in a semiconductor plant failed causing a release of chlorine gas. Investigation found that the unit was susceptible to conducted transients on the mains supply. There were no precautions against electrical interference in the power supply and the microprocessor watchdog was not effective in ensuring a safe state following detection of a fault. The UK manufacturer (Cambridge Fluid Systems) was successfully prosecuted under Health and Safety legislation.

Conclusions: It is not always recognised that a control system is safety-related. Microprocessor watchdog circuits are difficult to design for safety-critical applications, and should be supported by hardware and software EMC design techniques.

7.12 Traction current interference to safety circuits

Track circuits that detect the presence of a train on the 750V dc electrified lines of the former Southern Region use alternating current at the mains frequency of 50Hz. While the three-phase inverter drives for the traction motors in Networker and Eurostar trains are designed to minimise this frequency in the earth currents which return through the rails, there is the possibility that a drive could malfunction and interfere with the track circuits.

To protect against such a situation, the trains are fitted with an Interference Current Monitoring Unit (ICMU). If it detects a current at 50Hz above a certain threshold for more than 450ms the ICMU shuts the drive down.

Because Eurostar power cars are ... particularly prone to arcing when crossing gaps ...they generate interference at all frequencies, causing the ICMU to operate. To overcome this problem about 1,600 track circuits in the London area have had to be modified to be either immune to interference or to react more slowly. As a result the Eurostar ICMU can now be set to a two second delay and ...can run ... between London and Dollands Moor without the ICMU tripping.

Ref: Modern Railways, Nov. 1994, p653

Conclusions: Thanks to the rigorous fail-safe culture of rail engineers, no rail accidents have been attributed to poor EMC. The cost of this avoidance is large, as may be seen from the above extract.

7.13 Minor collision at sea due to a walkie-talkie

There was a minor collision between a supply vessel servicing a semi-submersible offshore oil and gas installation. The vessel experienced a sudden power increase brought on because of interaction between radio signals from a portable VHF radio and the joystick control. This caused the joystick to execute commands not requested by the operator and resulted in contact between the vessel and the installation. The interaction caused minor damage (though it could have been far worse).

The incident occurred outside UK waters and was reported in a safety notice issued by an offshore operator. The safety notice was seen by an HSE inspector on a bulletin board on an offshore installation, dated 30 September 1999, which referred to the incident as having happened 'recently'.

Conclusions: When failure of electronic control equipment to operate as intended could lead to injury or damage to health of people, the use of portable radio transmitters such as CB, walkie-talkies, or cellphones in close proximity to the equipment should be carefully assessed.

It may be necessary to impose restrictions on the use of such radio equipment, but remember that people do not always read notices or follow instructions, especially when under time pressure. So where a high safety integrity level is required it may be necessary to take special precautions in the design and installation of the control equipment to provide protection against the high levels of RF fields which exist close to portable radio transmitters.

7.14 Computer failure results in potential risk to operators

One of a number of computers controlling a chemical plant failed, resulting in the inappropriate setting of a number of process valves. Operating staff were potentially put at risk, as an opportunity existed for molten polymer to be discharged from pressurised autoclaves onto the casting floor before the normal casting operation. Investigation revealed that an integrated circuit had failed in the microprocessor which controlled the operation of an input/output interface. The failure meant that the processor set all signals for the output devices to logic 1 (all valves open).

The mains supply at this works suffered from high levels of transient interference which the power supply regulator of the interface power supply was not specified to handle. The voltage regulator eventually failed, which in turn caused the failure of the integrated circuit in the processor.

Failure of a microprocessor had been anticipated in the original design of the computer system, but the failure detection mechanism contained a design flaw. Fault detection was by a 'watchdog' circuit configured to trip when a status 'bit' flipped to zero – thereby indicating a physical failure of the processor. However, when the integrated circuit failed it set all bits, including the status bit, to logic 1 – the opposite to the state needed to trip the watchdog, so the failure was not recognised. Subsequent investigation also revealed that there were over 90 defects in the software, although none played a part in this particular incident.

Comment: The root cause of this incident was that computer control had been superimposed upon an existing plant previously controlled by traditional technology. No hazard and risk analysis had been carried out before this change, and no safety integrity requirements specification had been developed. The company carried out a detailed investigation into this incident with a hazard and operability study (HAZOP), which included examining in detail the failure modes of the computer, and their effects on the system as a whole.

An important finding of this HAZOP was that the computer or programmable system should be studied at the same time as the process design, not in isolation or retrospectively. Further advice on the inclusion of computer failure modes in a HAZOP study can be found in "*Guidance on HAZOP procedures for computer controlled plants*", HSE Books 1991, ISBN 0 7176 0367 9.

Also, the costs of this study, and those of implementing its findings, were estimated to be ten times those which would have been incurred if the work had been done within the original project.

The plant was re-commissioned under computer control only after the quality of the mains power had been improved, the defects discovered in the software corrected, and the fault detection scheme improved. The watchdog circuit was now configured to recognise a sequence of bits specifically generated each cycle to check the operation of the interface processor

Ref: "*Out of control. Why control systems go wrong and how to prevent failure."* HSE Books 1995, ISBN 0 7176 0847 6) p18-19.

Conclusions: Some mains supplies are 'polluted' with higher levels of transients than would normally be expected, and these may be higher than are covered by EMC standards harmonised under the EMC Directive and used when CE marking.

Users need to make sure that their supplies are not excessively polluted (refer to Annex B for more this topic) and manufacturers need to make sure that mains-powered equipment used for safety-related functions will withstand atypical mains transients as much as is reasonable, and when damaged by a transient (or suffer any other failure) will fail to a safe state.

8. Summaries of the industry annexes

8.1 Introduction

This report includes a number of 'Industry Annexes' which describe how various industries have addressed the issues of EMC-related functional safety.

Some of these annexes propose procedures for industries which do not control EMC-related functional safety very well at present.

All these annexes have been written by experts in those industries, with assistance from the entire team involved with this report.

Not all industries are represented here, but it is hoped that a sufficient cross-section has been provided that readers will be able to find one which is closely related to their own situation and needs.

It is hoped in the future to update these Annexes by modifying the existing ones and adding new ones.

Here are brief overviews of each annex to help readers select which annexes will be the most relevant.

8.2 **Aerospace** (Annex A)

The aerospace industry has long been aware of EMC-related functional safety issues, due to their long-term use of electronics in mission-critical and safety-critical applications – such as autopilots and automatic landing systems. The modern aircraft is vitally dependant on electronics, even for manual controls (e.g. in 'fly-by-wire' systems the pilots movements of his controls are mediated by computers and servo-systems before being applied to the aircraft systems or control surfaces).

All aircraft are exposed to very powerful EM disturbances, e.g. from airfield radars, radio broadcasting transmitters, and direct lightning strike. Military aircraft have the additional burdens of electronic warfare and countermeasures.

EMC in the aircraft industry involves the application of continually-evolving comprehensive standards which attempt to cover all foreseeable exposure to EM disturbances, including low-probability events, plus strict project management procedures for controlling EMC specification, design, development, and verification (e.g. testing).

8.3 **Building services and electricity distribution** (Annex B)

This annex consists of two conference papers written by ERA, aimed at Electrical Supply Managers and Facilities Managers, but also relevant to equipment manufacturers. They give an indication of what electrical equipment (apparatus) can expect in terms of disturbances on the power supplies, what typical effects these disturbances have, and what can be done to prevent potentially disruptive, expensive and harmful results. Voltage dips, dropouts, and interruptions of the supply are shown to be especially problematic, and barely controlled at all by existing standards.

Paper 1: The impact of International and European Standards upon Power Quality

Describes the typical disturbances covered both by EMC and mains supply standards, and differences between the standards are highlighted. The summaries provided here are a useful reference for manufacturers unsure of what disturbances their apparatus might be exposed to.

The conclusion is that whilst EMC standards are useful, equipment complying with them will not necessarily be immune enough to function correctly under many of the disturbances that can be considered normal, if infrequent, on their mains power supply. Voltage dips, dropouts, and interruptions are especially poorly covered by standards.

Paper 2: Achieving Quality and Reliability of Supply in Modern buildings

Starts from the same base as the first paper but considers more specific items. The foreseeable effects on a number of pieces of apparatus, and the disturbances created by typical building loads are considered, showing what can generally be expected. Some safety implications of incorrectly specified equipment are described, and some example solutions are provided. Voltage dips, dropouts, and interruptions are singled out for concern.

This paper concludes with a general approach to identifying and resolving power quality problems, including recommendations for both new and existing equipment. The overriding recommendation is to take a holistic system approach to power supplies, power quality and equipment specification, and continually monitor to ensure that the required levels of power quality are being achieved and the entire system is operating with the reliability necessary to achieve the desired level of safety.

8.4 **Healthcare** (Annex C)

The Medical Devices Directive (MDD), and the related Active Implantable Devices Directive, have recently been introduced in the EU. These cover the safety of medical devices that may come into contact with patients, and include requirements for manufacturers of such products to take EMC-related functional safety into account, as well as EMC in general.

A number of EMC-related safety incidents have been investigated and verified, principally by the USA's Food and Drug Administration (FDA), and these have caused considerable concern among healthcare professionals especially in the USA and Canada, where healthcare employs large numbers of electronic devices, products, and systems.

An EMC harmonised standard exists under the MDD, but this may not be adequate for controlling EMC-related functional safety, so the approach described in section 4 of this guidance document should be followed.

8.5 **Marine transport** (Annex D)

To account for the effects of EMC in the marine industry the hazard and risk assessment considers the specific EMC environment. The chief sources of interference above deck are the ship's own radio transmitters. The most susceptible equipment is the ship's radio receivers. The rationale, particularly for the bridge, is that definition of the limits of emissions and immunity for the radio equipment will allow compatibility. These limits set for other equipment in and around the bridge will allow compatibility of all electrical and electronic equipment in those areas.

For the rest of the ship, the assessment of EMC risk has been built into the Rules for Ship Classification Societies. The process identifies essential services and safety critical systems, further identifies programmable systems and other vulnerable items and requires a formalised type approval procedure which includes EMC testing.

8.6 **Offshore oil and gas** (Annex E)

The Offshore Industry as a whole has no formal procedure as yet. It is left to individual project managers or companies to identify and deal with this issue, with variable results. The industry is under cost and time pressure to accept CE marking to the EMC Directive as the only consideration necessary in respect of EMC. This guidance document shows that this practice can lead to increased hazards and risks.

This Annex recommends an engineering approach to EMC-related safety based on:

a) Assessing the EM environment for each installation

b) Specifying appropriate EM performance and validation requirements for offshore installations

c) Ensuring that all new projects meet these EM requirements by inclusion in the formal Safety Case assessments

d) Adopting design, installation and operating procedures for all new projects in accordance with latest EMC best-practices and suppliers requirements

e) Validating EM performance for safety-critical functions on-site as a necessary acceptance condition.

8.7 **Rail transport** (Annex F)

Guided transport systems use electrical energy for many different purposes. High powers are used for electric traction whilst very low powers are used for signaling and control purposes. The system will also be subject to interference from external sources and it may interfere with other external equipment. The EM environment of a guided transport system is complex and it is vital for the safe operation of such a transport system that the integrity of the signaling and control systems is not compromised by interference. The issue of EMC and functional safety is therefore of vital importance to the operators of such networks.

The Safety Case provides the prime assurance that the system is safe and an important part of the overall Safety Case for a guided transport system is a consideration of EMC issues. Any engineering or operational change can change the EM environment of the system and thereby affect functional safety. It is therefore vital that such issues are considered whenever change is implemented. These issues may be internal to a given system, e.g. within a locomotive or electricity supply sub station; or they may occur at system interfaces e.g. between traction and rolling stock and the signalling and communications systems.

The impact of external electrical networks and apparatus on the transport system and the impact of the transport system on external electrical systems must also be considered. Formal procedures must be used to identify and analyse relevant issues and to ensure any necessary control measures are adequate to ensure system safety. These procedures are outlined in this Annex.

8.8 **Road transport** (Annex G)

The automotive EMC environment is one of the most severe and the most unpredictable. Road vehicles are inherently mobile and thus able to drive near to any fixed transmitter. Vehicle owners and operators believe it to be their right to attach any sort of transmitter (even very high-powered ones) to the vehicle while expecting it to function correctly. Owners also expect to be able to fit electronic equipment into the vehicle and power it off the vehicle's power supply. Road vehicles do not generally fall under Directive 89/336/EEC but instead have their own product-specific EMC Directive, 95/54/EC. Although this adequately covers the fixed transmitter situation, it does not effectively deal with the possibility of mobile transmitters being installed on the host vehicle. Conducted transients are excluded from 95/54/EC since they are internal to the vehicle itself; however, this does not take into account the fitting of aftermarket accessories. ESD requirements are also excluded from 95/54/EC.

Despite the safety-related nature of vehicle EMC, at the time of writing, the author of this section of the report was not aware of any vehicle accidents being caused as a result of an EMC problem. This is almost certainly due to the fact that vehicle manufacturers, driven by product liability legislation, go to enormous lengths to ensure that their vehicles will not suffer from EMC problems.

Avoidance of EMC problems is achieved by a combination of tight specifications (both vehicle and sub-assembly), tight control of sub-assembly suppliers, good design, extensive testing of both vehicles and sub-assemblies, and by regarding the Automotive EMC Directive as being inadequate to achieve EMC for safety-related systems.

8.9 **Software** (Annex H)

The design of software should be part of the design features for tolerance against EM disturbances, as required by IEC 61508 part 2. This annex reviews the recommendations of the automotive industry guidance (the MISRA guidelines) for dealing with EMC issues in embedded software.

Although intended for use in the Automotive Industry, these guidelines may be of great value in improving the robustness of embedded software in other application areas. They consider the possible effects of EM disturbances on the following:

- Digital and analogue inputs, including the special case of external interrupts
- Communications lines
- Corruption of various types of memory
- Loss of control of the processor
- Misinterpretation/disruption of micro-code and corrupted clock pulses
- Corruption of data, including that on address buses, and stack-pointer corruption
- Floating point co-processing
- Open and closed-loop control systems.

Software solutions are recommended for mitigating the effects of EMI which overcomes hardware defences. Specifically, software can be used for the following functions related to EM interference:

- Digital filtering of data
- Comparing of data with constant, or inferred values to identify errors
- Performing error detection and correction on data in memory
- Detecting and correcting errors in communications data
- Dynamically adjusting scaling to optimise signal-to-noise ratios
- Managing failures and safe-state transitions.

8.10 **Heavy Industry** (Annex J)

At the present time, most heavy industry projects are carried out by subcontractors, with little or no project control of EMC beyond specifying that apparatus is supplied CE marked and meeting all relevant Directives. However, the failure of electrical/electronic systems to achieve EMC in practice often results in commissioning delays, under-performance, unreliability and potentially unsafe plant and equipment. These problems are destined to escalate as the proportion of sophisticated, but inherently sensitive, electronics deployed in the heavy engineering industries continues to increase.

The presence of CE marking, or compliance with the EMC Directive or its harmonised standards cannot, on their own, ensure that such problems will be avoided – particularly in the demanding EM environments encountered in heavy engineering. Experience indicates that the best solution is to design-out EMC problems from the outset.

This procedure has been developed to provide top-down control of the EMC of heavy industry projects, and its use is proposed for controlling all aspects of EMC, including EMC and functional safety and occupational exposure to non-ionising radiation. It defines a process for the procurement of electrical/electronic apparatus to avoid unwanted electrical interference or undue susceptibility to interference. A simple form with supporting checklists, together with a database of generic measurements, are used to simplify the task of assessing the EM environment into which the proposed apparatus is to be installed. Another key feature is the use of a ‘Contract Requirement Specification for Electromagnetic Performance’.

9. A Brief introduction to EMC

A number of EM disturbances may be emitted, either conducted or radiated (or both), due to the operation of electrical and electronic apparatus. Natural events such as electro-static discharge and lightning also create EM disturbances. EM disturbances, when present in sufficient amplitude in a given environment, may affect the functionality of any electrical or electronic apparatus.

EMC is the discipline of achieving compatibility between the EM disturbances present in an environment, and the ability of apparatus to continue to operate with adequate functionality despite these disturbances (its EM immunity). This includes compatibility with communication systems, particularly those used for emergency use.

Advances in electronic technologies generally result in devices and equipment which is more likely to emit EM disturbances, and also to have reduced immunity to EM disturbances (all else remaining constant). Because advanced electronic technologies are being used very much more widely (especially so in safety-related areas), the difficulties of achieving EMC are increasing very rapidly indeed. The reliability of electronic apparatus, and therefore its functional safety, is becoming more questionable.

A list of all known EM phenomena follows. Standards harmonised under the EMC Directive only cover a subset of these phenomena, and do not cover reasonably foreseeable situations where other disturbances might be present, or where the disturbances they do cover are present with larger amplitudes than normal.

9.1 Continuous EM phenomena

a) Voltage variations in AC and DC supplies (e.g. brownout)

b) AC supply phase imbalance

c) Harmonics and inter-harmonics of the AC power supply (waveform distortion)

d) AC ripple on the DC supply

e) AC or DC power-frequency earth currents, common-mode voltages, electric and magnetic fields

f) Radiated and conducted frequencies, either as electric or magnetic fields, from DC to 400GHz (i.e. 4,000MHz)

9.2 Transient EM phenomena

a) Voltage dips, dropouts, flicker, and interruptions (on AC or DC power)

b) AC power frequency variation

c) Fast transient bursts, both conducted and radiated effects

d) Electrostatic discharge (from personnel, machinery, and/or furniture), both conducted and radiated effects

e) Voltage surges (unidirectional or oscillatory) on AC and DC power supplies and on all long cables (including telecommunications)

f) Damped oscillatory and pulsed electric and magnetic fields

g) Direct lightning strike

h) Nuclear EM pulse (NEMP)

For a list of EM immunity test standards, please refer to the IEC 61000-4 series.

9.3 How does electronic equipment behave when exposed to EM disturbances

Physical parameter measurements are often processed by analogue circuits, and these can suffer errors of up to ± 100%, depending on the susceptibility of the circuit and the level of disturbance it is exposed to, including such things as:

- Safe load indicators
- Controlled variables in exothermic reactions
- Control of vehicle speed
- Control of flow, temperature, pressure, weight, mass, etc.

Computer(-ised) equipment can suffer from:

- Display errors
- False key-presses, possibly leading to operational mode changes
- False data
- Incorrect operation of software (e.g. continually repeating a subroutine)
- Loss of data and/or program
- Total failure (often called a crash) which can leave control outputs in *any possible combination of states*

For more information on EMC and EM phenomena, please refer to the IEE's *FactFile on EMC*. Annex J also contains a useful table of EM phenomena.

10. Functional Safety is not addressed by the EMC Directive

There is a common misperception that all that is needed to control EM interference for all purposes in the EU is to manufacture (or purchase) apparatus which is CE marked and declared compliant with the EMC Directive [5]. Here are some basic reasons why this perception is incorrect:

- The EMC Directive does not use the word "safety" anywhere in its text
- The EMC Directive only covers normal operation and does not cover reasonably foreseeable faults, environmental extremes, operator errors, maintenance situations, or misuse – all considerations which are essential for functional safety
- Almost all the EMC standards harmonised under the EMC Directive either explicitly or implicitly exclude safety considerations
- All the EMC standards harmonised under the EMC Directive (or R&TTE Directive) cover a restricted number of EM disturbances, and their limits allow a finite probability of incompatibilities
- EMC Technical Construction Files (TCFs) can include significantly lower EMC performance (or lower confidence of performance) than would have been achieved had the harmonised standards been applied in full, also a Competent Body would not usually assess a TCF for safety

So, complying with the EMC Directive is not necessarily a guarantee of freedom from EM interference in real life operation, or of freedom from safety risks due to inadequate EMC. The fact that the EMC Directive does not address issues of functional safety has been acknowledged by the European Commission's SLIM III Team on page 8 of [19], and by the EC [20].

10.1 The lack of coverage of safety issues in harmonised EMC standards

It is understood that CENELEC were instructed by the European Commission not to include safety requirements when creating harmonised EMC standards. The currently available harmonised immunity standards *specifically exclude* increasingly common situations, such as the likelihood of proximity of walkie-talkies, cellphones, or radio-energy apparatus (known as ISM equipment and covered by the scope of EN55011).

The texts of the harmonised generic immunity standards EN50082-1 and EN50082-2 (used by many manufacturers when product standards do not exist) *specifically exclude* safety considerations. Product-specific immunity standards presently under development in IEC, ETSI and CENELEC, all use the generic standards as their basis and so do not provide any safety considerations.

Harmonised standards for EMC emissions often specifically exclude situations where particularly sensitive apparatus is used in proximity. Those standards which don't state such limitations use similar test methods and/or emission levels so may be assumed to have the same implications.

Safety may, in real life, depend upon correct operation of electronic apparatus when it is subjected to low-probability EM disturbances which are not covered by harmonised standards. Even the latest issues of the generic EMC standards (a big improvement over the original issues, but manufacturers do not need to apply them until 01.07.2001) only cover EM disturbances thought likely to be present.

The EM environment is continually changing with the use of new technologies, and so harmonised standards often lag behind real needs. For example, there is increasingly common use of cellphones, wireless LANs and other RF transmitters, and ever-faster computers. These frequently emit

significant levels of disturbances at frequencies above 1GHz, higher than the frequencies covered by even the latest issues of the harmonised immunity standards.

11. Legal Liabilities

11.1 Introduction

The purpose of this chapter is to explain how the concept of functional safety, as it relates to EMC, is approached from a legal perspective. Details of the precise obligations imposed by the EMC legislation are to be found in [18].

Note that only UK law is considered here. Laws in other countries may be different. Where a UK law is the national implementation of an EU Directive, it may be expected that its equivalent in other EU Member States will be similar – but since the legal systems in each Member State have grown up differently, some legal concepts may be interpreted differently. Expert legal advice is always recommended in any case, when operating in or supplying any country (including the UK).

11.2 Safety and Law

Engineers tend to define safety in precise relative terms. So, for example, the *term* safety is defined in section 11 of [10] as “The freedom from unacceptable risks of personal harm”. The concept of safety is more widely explained in that document as relating to the freedom from risks that are harmful to a person, or group of persons, either local to the hazard, nationally or even world-wide. It is implied that for the consequences of an event to be defined as a hazard i.e. a potential for causing harm, there is some risk to the human population and therefore safety cannot be guaranteed, even if the risk is accepted when judged against some criterion of acceptability.

Alternatively, engineers look at safety by considering the inherent risks when the product is in use. Risk can then be expressed more simply. So for example, the definition of "risk" in [11] is the “likelihood of an event occurring and its consequences”.

By comparison, politicians are even more imprecise. Politicians, like the public, believe a product is either "safe" or "not safe". Of course, it is politicians who make the law. The expression of "safety" in various laws is therefore, imprecise. What the law does not say (but an engineer would say) is if there is a risk of (a single) death associated with the product then you must spend less than £X to avoid that risk being present but if the sum required to be spent is more than £Y, you need not spend it. This however is the way organisations which make those decisions on a day-to-day basis (including the Department of Transport, nuclear industry, chemical companies and even the Health and Safety Executive) look at matters.

Legal liability can arise in one of two ways. Legal liability can be criminal in which case a prosecutor (usually the State) takes action against a defendant. If the defendant is found guilty, he or she can be fined or sent to prison. Alternatively, liability can be civil, in which case the wrongdoer can be sued for damages by the party who has suffered injury or loss. This section examines each of these scenarios in turn.

11.3 Criminal Liability

A breach of the EMC Regulations [5], as with a breach of any of the other ‘CE marking legislation’ can give rise to a criminal liability. In England and Wales, the maximum penalty is a £5,000 fine and in the case of an individual, imprisonment of up to 3 months. [Note: in most European countries a criminal offence is committed by a breach of the CE marking legislation. However, in some countries a different approach is taken. For example, in Sweden, the primary method is by ordering a compulsory product recall in respect of non-compliant products.]

The EMC Regulations clearly impose specific duties relating to EMC on any person who supplies or 'takes into service relevant apparatus'. What is perhaps not so clear is that other product supply ('CE marking') legislation may also be relevant in the context of EMC. For example, The Supply of Machinery (Safety) Regulations [12] require that:

- '…the interruption …or fluctuation in whatever manner of the power supply to the machinery must not lead to a dangerous situation…', and:
- '…machinery must be so designed and constructed that external radiation does not interfere with its operation…', and:
- '…control systems must be designed so that …they can withstand …external factors…', and:
- '…errors in logic do not lead to dangerous situations…'.

Also, the Low Voltage Electrical Equipment (Safety) Regulations [14] require that:

- '…electrical equipment must be resistant to non-mechanical influences in expected environmental conditions, in such a way that persons, domestic animals and property are not endangered…'.

In addition, the Radio Equipment and Telecommunications Terminal Equipment Regulations [14bis] have an Essential Requirement with regard to:

> 'the protection of the health and safety of the user and any other person, including the objectives with respect to safety requirements contained in [the Low Voltage Directive] but with no voltage limit applying'.

In these examples, a failure to comply would mean not only that the manufacturer has produced a non-compliant product, but also that that he has produced an 'unsafe' product.

In addition to the specific product supply legislation, the Health & Safety at Work etc. Act 1974, places duties on manufacturers and suppliers of equipment intended for use at work and on employers and employees. A breach of this Act can lead to an *unlimited fine* or imprisonment for up to 2 years. The Health & Safety at Work etc. Act is very wide-ranging and could be applied in a number of ways in relation to EMC. For example:

- Employers are required to '…provide plant that (is) so far as is reasonably practicable, safe and without risks to health'. If an employer had knowingly provided equipment for use by employees which resulted in a dangerous situation because of an EMC related failure, then this could be considered to be a breach of this requirement. In most situations, an employer who ensures that equipment complies with the relevant product supply ('CE marking') legislation will be considered to have done what is 'reasonably practicable' *but this does <u>not</u> imply that meeting the EMC Directive is sufficient on its own to ensure that EMC-related safety issues have been fully addressed*.
- Employers are required to 'conduct (their) undertakings in such a way as to ensure, so far as is reasonably practicable, that persons not in (their) employment '…are not exposed to risks…'. An employer who, for example, knowingly continued to use equipment which was causing other equipment (not on his site) to malfunction due to an EMC problem, could be considered to be in breach of this requirement.
- Designers, manufacturers, installers or suppliers are required to design, construct, test and examine in such a way as to ensure that the equipment, so far as is reasonably practicable, is safe and without risks to health. Again, compliance with the relevant product supply ('CE marking') legislation is likely to be considered as adequate. However, they are also required to provide users of the equipment with any revisions of information that might be necessary to avoid a serious risk to health or safety.

This latter requirement is not covered by the product supply legislation and there has been at least one case [ref. to R v] which demonstrated the applicability of this requirement in the context of EMC. In this case, the supplier of a valve control panel used in a semiconductor manufacturing plant was found guilty of a breach of the Health and Safety at Work etc. Act (section 6 (1) (d)) because the supplier had failed to provide relevant information to the user when it became clear that a microprocessor 'watchdog' would not operate as designed, with the result that mains transients caused the equipment to fail in a way which led to a dangerous release of chlorine gas.

In addition to the Health & Safety at Work etc. Act there are several other more specific legal instruments which impose duties relating to the provision and use of work-place equipment and which might be relevant in the context of EMC. For example:

- The Provision and Use of Work Equipment Regulations, 1998, require that 'in selecting work equipment employers shall have regard to the working conditions and to the health and safety of persons…' and shall ensure that equipment complies with the 'CE marking' legislation.
- The Offshore Installations (Safety Case) Regulations as amended by the Offshore Installations and Wells (Design and Construction, etc.) Regulations, 1996 require independent competent verification of safety-critical elements. Such elements may include equipment which is potentially vulnerable to EM interference.
- The Offshore Installations (Prevention of Fire and Explosion, and Emergency Response) Regulations, 1995.
- The Control of Major Accident Hazard Regulations, 1999 (COMAH), which, for certain on-shore installations require that a safety report is produced which includes a description of how safety-related control systems have been designed to ensure safety and reliability.

11.4 Civil Liability

One source of civil liability is a breach of the statutory legislation in itself. There is a general principle of law that a breach of legislation such as the CE Marking legislation, or the Health and Safety at Work etc. Act 1974, will give rise to civil liability. This means that where a non-compliant product (that is one which does not comply with the CE Marking legislation) causes an injury, the person suffering the loss can claim damages.

This can arise where, for example, equipment that was supposed to be compliant (for example, equipment bearing the CE marking) interferes with another machine because the equipment bearing the CE marking is not, in fact, compliant. If the machine is permanently damaged, the owner of the machine can sue for damages. In certain limited circumstances, the owner of the machine may even be able to claim for the 'down-time' caused by the fact that he is unable to produce goods in his factory because the machine is not functioning. He can claim from the manufacturer of the equipment bearing the CE marking. In the same way, if the machine is interfered with in such a way that it causes injury to a third party, the third party can claim damages for his injury from the supplier of the non-compliant equipment.

However, there are other sources of liability from a civil perspective. These include the law of negligence (where the primary test is whether there has been a failure to take "reasonable" care) and breach of contract. Breach of contract claims are outside the ambit of this booklet, since each contract is likely to be unique. However, one common obligation found in contracts is an obligation to build equipment, "in compliance with applicable standards". Clearly such an obligation will mean that the equipment has to be built in accordance with the applicable EMC standards. Where this is not done and loss or injury occurs to the other contracting party, the other contracting party (i.e. the purchaser) can claim damages for breach of contract.

One problem from a contract law perspective is that it is only the purchaser who can bring a claim for loss or injury. Any other third party, who is not a party to the contract, must find another route to claim damages - such as for breach of statutory duty or negligence as discussed above. This is one of the reasons why the European Commission introduced the concept of product liability in 1985 [13].

11.5 Product Liability

Product liability is important because it imposes the highest duty on manufacturers of equipment. The manufacturer will be liable under the European product liability legislation if the manufacturer produces a product with a "defect" in it. The product is deemed to have a defect in it if it is not as "safe as people are generally entitled to expect". This standard is, in practice, a very high standard.

This can be seen by an analysis of the only useful defence under the legislation which is known as the "development risks" or "state of the art" defence. Although the defence has been worded slightly differently in English Law the (better) European Law is "that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered". From an analysis of this defence, it will be seen that only if everything is done that a typical manufacturer would do can the producer expect to have a defence.

In practice a typical producer can be expected to follow not only standards but draft standards. It may well be that a typical producer could follow not only good practice but best practice. If, therefore, best practice is not followed and as a result the product has a "defect" in it, liability will follow under the Product Liability Directive. Product liability legislation does not expose manufacturers to unending risk however, since the claimant may only claim for personal injury or loss of property of a personal (as opposed to a business) nature. Nevertheless, the product liability legislation imposes a high burden of duty on manufacturers from a safety perspective.

In certain circumstances, retailers can also be liable under the product liability legislation. The product liability legislation also catches importers of goods into the European Union.

11.6 Warnings

One issue that is common to all of these tests for safety is the extent to which warnings may be of assistance to a manufacturer in reducing his liability. In a similar manner, can a manufacturer avoid liability because the product he supplied has been misused? Although the precise rules are slightly different for each piece of legislation, in general the law is, sympathetic to these issues.

As was noted above, product liability imposes the highest safety obligations upon a manufacturer to ensure that the equipment does not produce hazards from an EMC perspective.

Product liability law requires a court to take into account:

- The use to which the product has been put (and whether the use is therefore reasonable or not)
- The instructions and warnings on the product, or any other way in which the product is presented
- Whether the product is designed for any particular class of individuals (for example, children)
- The safety standards prevailing at the time the product was supplied
- Any other relevant circumstances

However, it is very difficult, in practice, to "warn off" people from a dangerous product. Furthermore a strange use of a product may not necessarily amount to a misuse, if it is at least foreseeable by the manufacturer. Similarly, there is no point having a product which is perfectly safe in use but is dangerous when maintained. If the manufacturer expects the product to be maintained during its life, the manufacturer must plan *how* the product can be maintained in a safe manner during its life.

By the same principle, for example, the manufacturer of a computer would have great difficulty in saying that his product should not be used in medical applications, when, in reality, he knows that the computer is actually used widely in hospitals – in fact computer manufacturers do sometimes "attempt" to do just this! If the manufacturer of the computer wished to say this because he was worried about potential EM interference caused to other medical devices, he would not find the law sympathetic to his arguments.

The same principles holds, by and large for the criminal safety legislation i.e. for the CE Marking legislation. Indeed, in machine safety legislation, where some of these matters are expressly dealt with, it is expressly stated that, for example, a product must be safe, not only in use, but also in maintenance ([12] Annex 1 Section 1.6).

11.7 Standards

It needs to be considered whether or not compliance with standards is a sufficient defence from the perspective of the CE Marking legislation, or indeed any other legislation. Clearly it will only be a defence from a product liability perspective in so far as compliance with standards reflects good practice, or perhaps even best practice. This will not always be the case.

The CE Marking legislation that has been discussed not only looks at standards but requires some other additional mechanism, in order for a product to be considered "safe" from the perspective of that CE Marking legislation. For example, the machine safety legislation requires the product be built to the relevant safety standards *and* for it to meet the health and safety requirements set out in Annex 1 of [12]. In many circumstances compliance with standards will be insufficient because the standards are inadequate. They may be inadequate because they are old or because the legislation requires some further test to be passed: for example [12] also requires that the essential health and safety requirements set out in its Annex A are met.

Clearly, if the safety standard is old, compliance will not guarantee that there is no liability for incidents. Even where the standard is current, thought still needs to be given to risks that may not be adequately dealt with in the standard - see the case of Balding v Lew Ways Limited (The Times 9th March 1995). Therefore suppliers need to be certain that not only are they following all relevant standards but that the standards that they follow reflect "good practice".

11.8 Partial list of legislation

The following table is a partial list of CE marking legislation which concerns safety, which could be breached with either criminal or civil penalties if safety problems were caused by goods which either created too much EM disturbance for their actual user environment, or had insufficient immunity to their actual user EM environment.

Table 1 THE CE MARK LEGISLATION (partial)

(References to the relevant legislation are included in Tables 2 and 3)

SUBJECT	EU DIRECTIVES	IMPLEMENTING UK LEGISLATION
ELECTROMAGNETIC COMPATIBILITY (incorporating a special regime for telecommunications terminal equipment)	89/336[1] as amended by 91/263[2], 92/31[3] and 93/68[4]	SI 1992/2372[A] as amended by SI 1994/3080[B] and SI 1995/3180[H] SI 1992/2423[C] as amended by SI 1994/3129[D] as amended by SI 1995/144[E] and SI 1997/3051[II]
MACHINE SAFETY (incorporating a special regime for mobile machines and lifting equipment)	89/392[5] as amended by 91/368[6], 93/44[7] and 93/68[4] and 98/37[20] as amended by 98/7921	SI 1992/3073[F] as amended by SI 1994/2063[G]
LOW VOLTAGE EQUIPMENT	73/23[8] as amended by 93/68[4]	SI 1989/728[H] as revoked by amended by 1994/3260[I]
SIMPLE PRESSURE VESSELS	87/404[9] as amended by 90/488[10] and 93/68[4]	SI 1991/2749[J] as amended by SI 1994/3098[K]
TOY SAFETY	88/378[11] as amended by 93/68[4]	SI 1989/1275[L] as amended by SI 1993/1547ML[M] as revoked by SI 1995/204[N]
CONSTRUCTION PRODUCTS	89/106[12] as amended by 93/68[4]	SI 1991/1620[O] superseded by SI 1994/3051[P]
PERSONAL PROTECTIVE EQUIPMENT	89/686[13] as amended by 93/68[4] and 93/95[14] and 96/5822	SI 1992/2966[Q] and SI 1992/3139[R] as amended by SI 1994/3074[S], SI 1994/3017[AA], SI 1996/3039[BB], SI 1999/860[CC], and SI 1994/2326[T]
NON-AUTOMATIC WEIGHING INSTRUMENTS	90/384[15] as amended by 93/68[4]	SI 1995/1907[U] as amended by SI 1997/3035[DD] and SI 1998/2994[EE]
GAS APPLIANCES	90/396[16] as amended by 93/68[4]	SI 1992/711[V] as revoked by SI 1995/1629[FF] and SI 1996/2001[GG]
BOILER EFFICIENCY	92/42[17] as amended by 93/68[4]	SI 1993/3083[W] as amended by SI 1994/3083JJ
ACTIVE IMPLANTABLE MEDICAL DEVICES	90/385[18] as amended by 93/42[19], 93/68[4] and 98/79[21]	SI 1992/3146[X] as amended by SI 1995/1671[Y] and SI 1995/2487[KK] and SI 1997/694[LL]
MEDICAL DEVICES	93/42[19]	SI 1994/3017[AA]
IN-VITRO MEDICAL DEVICES	98/79[21]	L331/1 Pub. 7.12.98
RADIO AND TELECOMMUNICATIONS TERMINALS	99/5[23]	SI 2000/730[MM]

Table 2 EU DIRECTIVES

1	(89/336)	Council Directive on the approximation of the laws of the Member States relating to electromagnetic compatibility (O.J. 1989, L139/19)
2	(91/263)	Council Directive on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including the mutual recognition of their conformity (O.J. 1991, L128/1)
3	(92/31)	Council Directive amending Directive 89/336 on the approximation of the laws of the Member States relating to electromagnetic compatibility (O.J. 1992, L126/11)
4	(93/68)	Council Directive amending Directives 87/404, 88/378, 89/106, 89/336, 89/392, 89/686, 90/384, 90/385, 90/396, 91/263, 92/42 and 73/23 (O.J. 1993, L220/1)
5	(89/392)	Council Directive on the approximation of the laws of the Member States relating to machinery (O.J. 1989, L183/9)
6	(91/368)	Council Directive amending Directive 89/392 on the approximation of the laws of the Member States relating to machinery (O.J. 1991, L198/16)
7	(93/44)	Council Directive amending Directive 89/392 on the approximation of the laws of the Member States relating to machinery (O.J. 1993, L175/12)
8	(73/23)	Council Directive on the harmonisation of the laws of the Member States relating to electrical equipment designated for use within certain voltage limits (O.J. 1973, L77/29)
9	(87/404)	Council Directive on the harmonisation of the laws of the Member States relating to simple pressure vessels (O.J. 1987, L220/48)
10	(90/488)	Council Directive amending Directive 87/404 on the harmonisation of the laws of the Member States relating to simple pressure vessels (O.J. 1990, L270/25)
11	(88/378)	Council Directive on the approximation of the laws of the Member States concerning the safety of toys (O.J. 1988, L187/1)
12	(89/106)	Council Directive on the approximation of laws, regulations and administrative provisions of the Member States relating to construction products (O.J. 1989, L40/12)
13	(89/686)	Council Directive on the approximation of the laws of the Member States relating to personal protective equipment (O.J. 1989, L399/18)
14	(93/95)	Council Directive on the approximation of the laws of the Member States relating to personal protective equipment (PPE) (O.J. 1993, L276/11)
15	(90/384)	Council Directive on the harmonisation of the laws of the Member States relating to non-automatic weighing instruments (O.J. 1990, L189/1)
16	(90/396)	Council Directive on the approximation of the laws of the Member States relating to appliances burning gaseous fuels (O.J. 1990, L196/15)
17	(92/42)	Council Directive on efficiency requirements for new hot-water boilers fired with liquid or gaseous fuels (O.J. 1992, L167/17)
18	(90/385)	Council Directive on the approximation of the laws of the Member States relating to active implantable medical devices (O.J. 1990, L189/17)
19	(93/42)	Council Directive concerning medical devices (O.J. 1993, L169/1)
20	(98/37)	Council Directive on the approximation of the laws of the Member States relating to machinery (O.J. 1998, L207/1)
21	(98/79)	Council Directive on in vitro diagnostic medical devices (O.J. 1998, L331/1)
22	(96/58)	Council Directive amending Directive 89/646/EEC on the approximation of the laws of the Member States relating to personal protective equipment (O.J. 1996, L236/44)
23	(99/5)	Council Directive on radio equipment and telecommunication terminal equipment (O.J. 1999, L91/10)

Table 3 IMPLEMENTING STATUTORY INSTRUMENTS IN THE UNITED KINGDOM

A	Electromagnetic Compatibility Regulations 1992
B	Electromagnetic Compatibility (Amendment) Regulations 1994
C	Telecommunications Terminal Equipment Regulations 1992
D	Telecommunications Terminal Equipment (Amendment and Extension) Regulations 1994
E	Telecommunications Terminal Equipment (Amendment) Regulations 1995
F	Supply of Machinery (Safety) Regulations 1992
G	Supply of Machinery (Safety) (Amendment) Regulations 1994
H	Low Voltage Electrical Equipment (Safety) Regulations 1989
I	Electrical Equipment (Safety) Regulations 1994
J	Simple Pressure Vessels (Safety) Regulations 1991
K	Simple Pressure Vessels (Safety) (Amendment) Regulations 1994
L	Toy (Safety) Regulations 1989
M	Toy (Safety) (Amendment) Regulations 1993
N	Toy Safety Regulations 1995
O	Construction Products Regulations 1991
P	Construction Products (Amendment) Regulations 1994
Q	Personal Protective Equipment at Work Regulations 1992
R	Personal Protective Equipment (EC Directive) Regulations 1992
S	Personal Protective Equipment (EC Directive) (Amendment) Regulations 1993
T	Personal Protective Equipment (EC Directive) (Amendment) Regulations 1994
U	Non-Automatic Weighing Instruments (EEC Requirements) Regulations 1992
V	Gas Appliances (Safety) Regulations 1992
W	Boiler (Efficiency) Regulations 1993
X	Active Implantable Medical Devices Regulations 1992
Y	Active Implantable Medial Devices (Amendment and Transitional Provision) Regulations 1995
AA	Medial Devices Regulations 1994
BB	Personal Protective Equipment (EC Directive) (Amendment) Regulations 1996
CC	Police (Health and Safety) Regulations 1999
DD	Non-Automatic Weighing Instruments (EEC Requirements) (Amendment) Regulations 1997
EE	Non-Automatic Weighing Instruments (EEC Requirements) (Amendment) Regulations 1998
FF	Gas Appliances (Safety) Regulations 1995
GG	Mines (Substances Hazardous to Health) Regulations 1996
HH	Electromagnetic Compatibility (Amendment) Regulations 1995
II	Electromagnetic Compatibility (Wireless Telegraphy Apparatus) Certification and Examination Fees Regulations 1997
JJ	Boiler (Efficiency) (Amendment) Regulations 1994 - amended by Directive 93/68 which implements Directive 92/42
KK	Medical Devices Fees Regulations 1995
LL	Medical Devices Fees (Amendment) Regulations 1997
MM	Radio Equipment and Telecommunications Terminal Equipment Regulations 2000

12. Making a case for safety – a wide range of options

The amount and quality of the actions and documentation required to be able to demonstrate that an apparatus is as safe as its users and third parties have a right to expect can vary significantly from one organisation to another. In general, where hazards and risks are higher (i.e. a higher safety integrity level applies), a higher level of activity and documentation is required.

This section lays out guidelines for safety 'arguments' which may be adapted to a very wide range of organisations, from 'one-man bands' through small and medium sized enterprises to large organisations.

(Section 13 describes the more formalised 'safety case approach' that has been developed by large organisations building safety-critical systems such as rail networks, to satisfy the requirements of the HSE.)

12.1 General

The purpose of a safety case is usually to:

- Set out a clear, concise, correct and consistent set of arguments that the risks relating to the development and deployment of a Safety-Related System (SRS) have been reduced to a level that is tolerably low; and
- To provide evidence which adequately supports each strand of the argument.

In this context, the term *safety related* applies to a system if that system is performing a (safety) risk-reduction function and/or failure of the system would cause an increase in safety risk. What is *tolerable* in terms of safety risk is normally determined by the safety policy applicable to the system.

There is an increasing trend for safety regulatory authorities to move away from an inspection role and instead to place the burden of proof on the 'regulatee' – i.e. the safety case must show positively and unequivocally that the system is tolerably safe, rather than 'challenge' the regulator to show that it is not safe!

Although there are a number of possible ways of setting out a safety case, the most important consideration is that all aspects of the lifecycle are covered adequately.

This section addresses those *argument/evidence* aspects of the five principal phases of a typical development life-cycle that are relevant to EMC:

a) Requirements determination

b) Design

c) Implementation (of the design)

d) Installation

e) Commissioning and integration

f) Transition to operational use

This section also outlines the types of EMC *evidence* which could be appropriate to a safety case and how it could be used.

12.2 Requirements determination phase

12.2.1 Concept of operations

Since the EMC threat to and from a deployed system is determined as much by its surroundings as from any of its intrinsic properties, it is essential that *evidence* be obtained to show that:

- The environment in which the system has to operate is clearly identified in terms of the electromagnetic disturbances to which the equipment may be exposed, and the other systems which might be affected by emissions from the system;
- The safety relevance of the use to which the system will be put is clearly and correctly defined and understood by those responsible for specifying the system's EMC safety requirements and for validating the completed system against those requirements.

If the system itself is not safety-related (is not an SRS) and is not intended for use in an environment in which it could adversely affect the operation of other SRSs, then there are no functional safety issues to be addressed.

12.2.2 Safety requirements specification

In general, safety requirements can be expressed two complementary forms:

- *Function and performance* (F&P) – these are the positive attributes of a system which specify what the system has to do and how well it needs to do it
- *Derived safety requirements* – these are the negative attributes of a system which specify what the system should not do and constrain the rate at which such undesired behaviours are permitted to occur

By their very nature EMC characteristics are undesirable and therefore fall entirely under the heading of *derived safety requirements*.

Evidence should be obtained to show that:

a) If the system is safety-related, then complete and correct EMC Safety Requirements have been specified which provide the system with adequate immunity to emissions from its surroundings

b) Complete and correct EMC Safety Requirements have been specified so as to limit the emissions from the system such that it cannot adversely affect the operation of any other SRS

c) Requirements have been properly and adequately specified which preserve the safety of the on-going service (to which the system relates) during the development, installation, commissioning, integration and transition activities relevant to the system

In all the above three cases, the requirements are derived from a hazard analysis which considers the threats to, and from, the system.

In many situations, it would be impracticable to specify the system such that the emissions from it could not adversely affect the operation of another SRS, because the environmental parameters and susceptibility characteristics of the latter system would be impossible to determine. In those cases, demonstration of compliance with accepted EMC standards in the specification, design and development of the system might be the best that can be achieved.

12.3 Design phase

Evidence should be obtained to show that:

a) The Design and Development process for the system has been fully documented in a form which is appropriate to the criticality of the specified EMC safety requirements

b) Full traceability exists between the EMC safety requirements and all levels of the system design

c) The system design fully meets the EMC safety requirements

d) The validation process, for demonstrating that the developed system meets the EMC safety requirements, has been adequately planned

12.4 Implementation phase

Evidence should be obtained to show that:

a) The system design and development process has been fully complied with, in respect of the EMC safety requirements

b) The system design and development process has been fully effective, in respect of the EMC safety requirements

c) The requirements for the factory aspects of the EMC safety validation plan have been adequately specified

d) The specified system factory EMC safety validation requirements have been met in full

e) The EMC aspects of the subsequent system installation, commissioning and integration activities will not adversely affect the safety of the on-going service

f) Any constraints on, and assumptions about, the operation and maintenance of the system, in respect of the EMC safety requirements, have been identified and have been shown not to detract from the ability to maintain the safety of the service that the system is intended to support

12.5 Installation, commissioning, and integration phase

Evidence should be obtained to show that:

a) The EMC safety aspects of the system installation, commissioning and integration requirements have been adequately specified

b) The EMC safety aspects of the system installation, commissioning and integration requirements have been satisfied

c) The on-site safety validation process for demonstrating that the installed, commissioned and integrated System meets the EMC Safety Requirements has been adequately specified

d) The on-site safety validation process for demonstrating that the installed, commissioned and integrated system meets EMC safety requirements has been completed satisfactorily

e) Any EMC-related dependencies on other systems, or limitations on the use of the system, have been recorded and appropriate measures taken to ensure that the safety of the system and/or service is not impaired

f) The operational and engineering implications of any shortfall in the system EMC characteristics have been assessed and have been shown not to detract from the ability to maintain the safety of the service

g) The EMC aspects of the subsequent transition of the system into operational use will not adversely affect the safety of the on-going service

12.6 Transition-to-operational-use phase

Evidence should be obtained to show that:

a) Engineering procedures in respect of EMC are in place for the safe normal and abnormal operation of the system

b) Engineering procedures in respect of EMC are in place for maintenance of the system

c) Appropriate corrective action has been taken to mitigate, or accept, any EMC safety requirements which have not been proven to be met

d) Any EMC safety aspects of the specialist operator and engineering training have been completed adequately

12.7 'Rules of evidence'

12.7.1 Introduction

Clearly, the adequacy of a safety case rests on the completeness and correctness of the *argument* and on the quality of the *evidence* to support the *argument*. One way of ensuring that evidence is adequate is to establish a set of rules, an example of which, based on categorisation of evidence, is outlined below.

12.7.2 Categories of Evidence

Evidence can be considered as falling into three complementary categories, as follows.

12.7.2.1 Direct Evidence

The best *evidence* to demonstrate, in a direct sense, that the System meets the EMC safety requirements is that obtained from testing. However, the nature of EMC problems – especially the mixture of random and systematic characteristics of the 'failure' modes and the unpredictability of the system's operational environment – means that testing alone will often not be adequate. In that event, other sources – e.g. field service experience and analysis – could also be a valid source of *direct evidence*.

12.7.2.2 Backing Evidence

It is usually also necessary to show that the *direct evidence* is soundly based and trustworthy. The term *backing evidence* is used to describe evidence that is intended to demonstrate that the *direct evidence* can be relied upon. For example, arguments and evidence that the testing regime is adequate and that the tests have been properly conducted would be necessary as *backing evidence* for the *direct evidence* obtained from testing.

12.7.2.3 Reinforcement Evidence

Where *direct evidence* alone is not adequate – principally when failure rate targets are more stringent (the safety integrity levels are so high) than can be demonstrated by testing alone – then *reinforcement evidence* is also required to show how the *direct evidence* can be extrapolated to provide additional assurance that the EMC safety requirements have been met.

12.7.3 Source of Evidence

Evidence of satisfaction of EMC Safety Requirements (i.e. validation) may be obtained from a number of sources, including:

a) Analysis – e.g. of frequency relationships

b) Mathematical modelling and simulations

c) System design – especially conformance with accepted standards, design techniques etc

d) System prototyping

e) Testing of the system in the factory

f) Installation design – especially conformance with accepted standards, design techniques etc

g) Proof of installation integrity – e.g. bonding measurements

h) Testing of the system on site – i.e. in its operating environment

i) Field service experience of previously deployed systems of the same design and construction

j) Influence of system integrity requirements

Although, as noted above, testing is the best form of *direct evidence*, the degree to which any of the various sources of evidence would be adequate for any of the three evidence categories would depend on the required safety integrity level of the system – i.e. the higher the required integrity, the more complete and rigorous the *direct evidence* needs to be and the greater the need for high quality *backing* and *reinforcement evidence*.

13. Brief review of safety case approaches for designers of equipment or large systems where safety is important

The amount and quality of the actions and documentation required to be able to demonstrate that an apparatus is as safe as its users and third parties have a right to expect can vary significantly from one organisation or situation to another. In general, where hazards and risks are higher (i.e. a higher safety integrity level applies), a higher level of activity and documentation is required.

This section briefly describes approaches to safety cases which has been developed by a number of safety-critical industries jointly with the HSE over many years. These tend to be used in the design of large engineering projects (e.g. rail networks) and are described here for information only (not as a complete safety case guide). The management and operation of the finished system is a separate issue.

(Section 12 lays out the general guidelines for safety 'arguments' which may be adapted to a very wide range of organisations, from 'one-man bands' through small and medium sized enterprises to large organisations.)

13.1 General

Safety is a design parameter or attribute, however it has a number of important aspects that separate it from the normal design parameters:

a) Safety can not be measured directly in the same way as other parameters until such time as the equipment/system is in service. Then a record of incidents can be formulated but by then it is not cost-effective to cure the problem/problems.

b) Nothing is safe and safety has no absolutes. However, it is possible to determine a level of tolerability for a risk that is acceptable. This level of tolerability may be determined by a customer or will need to be determined to suit the circumstances by the supplier/manufacturer.

c) Although it is possible to demonstrate, with a high degree of confidence, that safety requirements will be met within project timescales and cost constraints, there will be a lack data available on equipment/system operation. Data only becomes available as the equipment/system is taken into operation and at this time system/equipment safety can be seriously compromised if safety-related accidents occur. It is perhaps a truism that once data is available, the unacceptable has already happened.

d) The level of safety achieved depends directly on management involvement.

13.2 Introduction

In larger systems such as rail networks, when dealing with safety-critical systems (and in some cases to cover product safety liability) a safety case as outlined below is used to meet HSE requirements.

a) The safety case is not limited to EMC but covers a multitude of "sins". DEF-STAN 00-56 part 2 Annex B provides an excellent guide to the type of hazards (including EMC) that should be considered.

b) When dealing with safety-critical systems, it may be that a safety case has already been adopted, and that only the inclusion of EMC is required.

c) This approach taken to its fullest is a well disciplined formal approach to safety, but, in order to meet the requirements of your product/system you may not need to adopt the full formal approach (refer to Section 12).

The objective of a safety case is to set up a system/equipment safety programme to ensure that a level of safety consistent with the intended usage is designed-in.

13.3 Safety management

13.3.1 Safety programme plan

The safety programme plan is a document created early in the programme, or even as part of the tender documentation. The safety experts, rather than EMC engineers, should raise this document. It will cover such areas as:

a) Organisation structure to cover safety and lay down levels of responsibility

b) Definition of the stages of the safety programme, especially where it integrates with design development, production, integration and other support activities

c) Reference to all internal procedures, national, and international standards to be used. This should include the techniques to be used such as Fault Tree Analysis, Failure Modes and Effects Analysis (FMEA), etc.

d) Analysis and assessments, including details on how the hazard analysis will be approached and the considerations that will affect the decisions made

13.3.2 EMC activities

At this point an EMC control plan should be raised as an input to the project management and the safety programme plans.

The purpose of the EMC control plan is to provide clear EM control guidelines to technical management, design and test engineers such as to ensure compliance with the Project Requirements.

This plan will cover such topics as:

a) Project EMC control

b) Creation of a safety log to identify EMC hazards

c) Analysis of project requirements

d) Hazard analysis

e) EM environment analysis

f) Application of EMC standards

g) EMC design controls to identify how EMC and hazards will be controlled

h) EMC test requirements

i) Documentation requirements

13.3.2.1 Project EMC control

This section will cover the organisation structure to cover safety and lay down levels of responsibility. It will define the stages of the EMC programme, especially where it integrates with design, development, production, integration and other support activities.

The instigation of a working group consisting of the system EMC engineer, delegated equipment engineers, the project system engineers and a safety expert is recommended. This group should hold regular meetings to discuss project progress with the emphasis on EMC and EMC hazards.

The system EMC engineer will hold regular review meetings with subcontractor/supplier EMC controllers in order that information flows both upwards and downwards. These design reviews will be timed to coincide with engineering design reviews or their equivalent and will provide a forum that will enable changes in philosophy to be discussed and agreed or passed on.

These meetings will ensure that any overall system requirements are reflected and implemented throughout the project.

13.3.2.2 Analysis of project requirements

The requirements of the project must be fully analysed. At the same time the system/equipment design, hardware, software and interfaces must be fully understood and assessed against the project requirements.

13.3.2.3 Analysis of the EM environment

A complete assessment of the EM environment at the intended location of the system should be made. This assessment should be as full as possible and cover such areas as:

a) Radiated EM field disturbances (both near and far fields)
   This should cover both continuous and transient disturbances, and ESD

b) Conducted EM disturbances
   This should cover both continuous and transient disturbances and ESD, as well as surges

All sites should be assessed and, if considered necessary, site ambient measurements should be made.

13.3.2.4 Application of EMC standards

Many EMC specifications and standards are directed toward establishing limits on individual units, and by themselves do not guarantee any specific degree of compatibility when the units are assembled as part of a larger system. A particular limit may be set too low thereby causing devices to be very susceptible to their EM environment, or be set too high thus causing unnecessary expenditure to overcome non-existent hazards.

Based on the analysis in 13.3.2.3 and the controls to be implemented in 13.3.2.5 it may be possible to tailor the test levels and limits of the standards that are to be used or placed on suppliers (it should also be borne in mind at this time any requirements for CE marking).

13.3.2.5 EMC design controls

These should follow good design practice for EMC, but special care should be taken to ensure that design engineers are aware of any special requirements to control identified EMC hazards.

13.3.2.6 Test requirements

Based on the analysis and information derived from 13.3.2.3 and 13.3.2.4 it may be considered that not all potential EMC hazards are covered. Therefore it may be necessary to perform extra tests on the equipment/system. Also at this time the operational parameters of the equipment/system should be defined:

- Is it permissible for the equipment to stop working during the application of the disturbance?
- Must the equipment work correctly under all circumstances?
- If the equipment fails, is it necessary for it to fail in a safe condition?

13.3.2.7 Documentation requirements

Define the level of documentation required. The level required is dependent on the end result and the means by which the system/equipment is designed.

If it is a system making use of commercial-off-the-shelf (COTS) units then Declarations of Conformity for CE marking may not be enough and full reports may be required. When analysing the EM environment the reports on each equipment will be useful in determining any margins available or the extra protection that needs to be built into the system.

For example, in some test laboratories it is normal to test at levels above those required to meet the immunity standard, only backing off the power where susceptibilities occur. If this has been done and the equipments involved have all been adequately over-tested when compared with the EM environment, then further 'hardening' (improvements in immunity performance) may not be necessary. Conversely if the equipment only just meets an environmental requirement then further work will be required to harden the equipment or system.

If the equipment or system is bespoke, reports must be produced to show that the safety aspects and hazards have been fully addressed.

13.4 Hazard analysis

13.4.1 System/equipment boundary

The first step, before starting the hazard analysis, is to provide terms of reference to the description of the system/equipment limits, its boundary and its intended use. A clear description is needed at this stage in order to avoid confusion at a later stage, for example if the system/equipment is to be interfaced with other machinery or transfer systems.

13.4.2 Identification of hazards

The identification of hazards and hazardous situations is the most important step in any safety case study because any hazard omitted at this stage will lead to the associated risk not being assessed.

It is important to distinguish between continuing hazards (those inherent in the work activity or equipment under normal conditions) and those hazards which can result from failure or error (e.g. hardware or software failures as well as foreseeable human error). Also not to be overlooked is the possibility of intentional misuse. These two types of hazard will need to be addressed separately as hazards resulting from failure will need more sophisticated identification techniques (see below).

There are several qualitative hazard identification techniques, which provide a formalised and structured procedure. Selection of the appropriate procedure will depend on the type of system/equipment and the hazards involved. Procedures may range from simple checklists to a more sophisticated analysis dependent on the complexity or requirements.

The identification of hazards and hazardous situations must be approached with care and will need expert knowledge of the system/equipment, its operation, intended environment, maintenance and disposal. This means that it will have group involvement taken from all necessary disciplines, as well as representation from the management (project or company) levels.

13.4.3 Hazards resulting from failure, human error or misuse

Hazards resulting from equipment failure, human error or misuse require:

a) A detailed hazard identification to be carried out for all stages of the system life-cycle – from the concept phase to design, installation, commissioning, use, maintenance and final decommissioning phases

b) Analysis of systems of work and established procedures to identify who might be exposed to a hazard and when – e.g. operator under normal conditions, maintenance worker, tool fitter, cleaner, member of public, etc.

13.4.4 Hazard identification techniques

Structured and systematic techniques that would assist in the identification of these hazards might include the following:

13.4.4.1 Hazard and Operability study (HAZOP)

A qualitative technique to identify hazards resulting from hardware failures and human error.

13.4.4.2 Failure Modes and Effects Analysis (FMEA)

An inductive technique, which starts at the component level ('bottom-up' approach) to identify and analyse hardware failures. This technique is extremely useful as it provides means for risk quantification.

But there are problems with FMEA techniques:

- Tables of component failure rates might not include EMC-related failures
- The usual calculation process does not take account of the possibility that common-cause failures (which can easily happen where EMC is inadequate) can reduce the reliability of multi-channel redundant systems to that of a single channel.

13.4.4.3 Task analysis

A deductive technique to identify systematically what should be done, and when. This technique, based on a 'top-down' approach, can be used to identify opportunities for different types of human error. Task analysis begins by stating the objective of a certain operation or maintenance task, then breaks down this task into steps or actions in a structured way.

13.4.4.4 Other useful techniques

- Brainstorming
- Fault Tree Analysis (FTA)
- Investigates causes and consequences of known top events (Hazards)
- Procedural analysis
- Analyses the human interaction with the product or system
- Check lists
- Problem Identification Game (“PIG”)

13.4.5 Potential EMC Hazards

Refer to section 9 and the useful table of EMC disturbances in Annex J

13.4.6 Affected areas

- Interfaces(in particular safety-related) between the various elements of the system
- Disturbances from or to the operating EM environment

Amended 04.01.01

13.5 Risk Analysis

Having determined all the potential hazards, the level of risk or tolerability associated with each one is now determined. This broadly categorises the severity and the probability of each identified hazard. Generally descriptive terms are used, rather than mathematics (unless otherwise required by the customer/contract or the standard being used). There may be a need for Quantified Risk Analysis (QRA), and this is the trend for regulatory authorities and standard bodies.

13.5.1 Severity

As previously stated it is not always possible to give quantifiable rates to different categories, however the descriptions given below are typical for severity ratings:

1) Catastrophic Death(s), system loss, or major environmental damage
2) Critical Serious injury or illness, major system or environmental damage
3) Marginal Minor injury or illness, or minor system or environmental damage
4) Negligible Trivial injury, or trivial environmental damage

13.5.2 Probability

The following are typical descriptions for probability:

A) Frequent Several times per day or mission. Many times in each product's lifetime
B) Probable Maybe once per day or per mission. Several times in each product's lifetime
C) Occasional Happens sometimes. Could well occur at least once in each product's lifetime
D) Remote Might perhaps occur in each product's lifetime
E) Improbable Unlikely to occur

13.5.3 Risk Matrix

Once the severity and probability of each hazard is determined, the acceptability of the resulting risk is assessed. Figure 1 gives an example of a typical hazard risk assessment matrix. Levels of acceptable risk will vary from project to project, and from company to company.

FIGURE 1 Example of a Risk Matrix H = High risk, M = Medium risk, L = Low risk

		PROBABILITY				
		A	B	C	D	E
		FREQUENT	PROBABLE	OCCASIONAL	REMOTE	IMPROBABLE
SEVERITY	1) CATASTROPHIC	H	H	H	H	H
	2) CRITICAL	H	H	H	M	M
	3) MARGINAL	H	H	M	L	L
	4) NEGLIBLE	M	L	L	L	L

If the risk is too high then steps to mitigate the problem must be taken. The earlier in the design cycle this decision is made the less cost impact it is likely to have.

For medium risks a more detailed analysis may be required to determine whether this level of risk is acceptable to the company or project. It is recommended that a senior member of the company, or if necessary the customer, be involved with this level of decision.

Low risks may be considered to be a tolerable risk, however if they can be controlled at an acceptable level of cost, then they should be.

13.5.4 ALARP

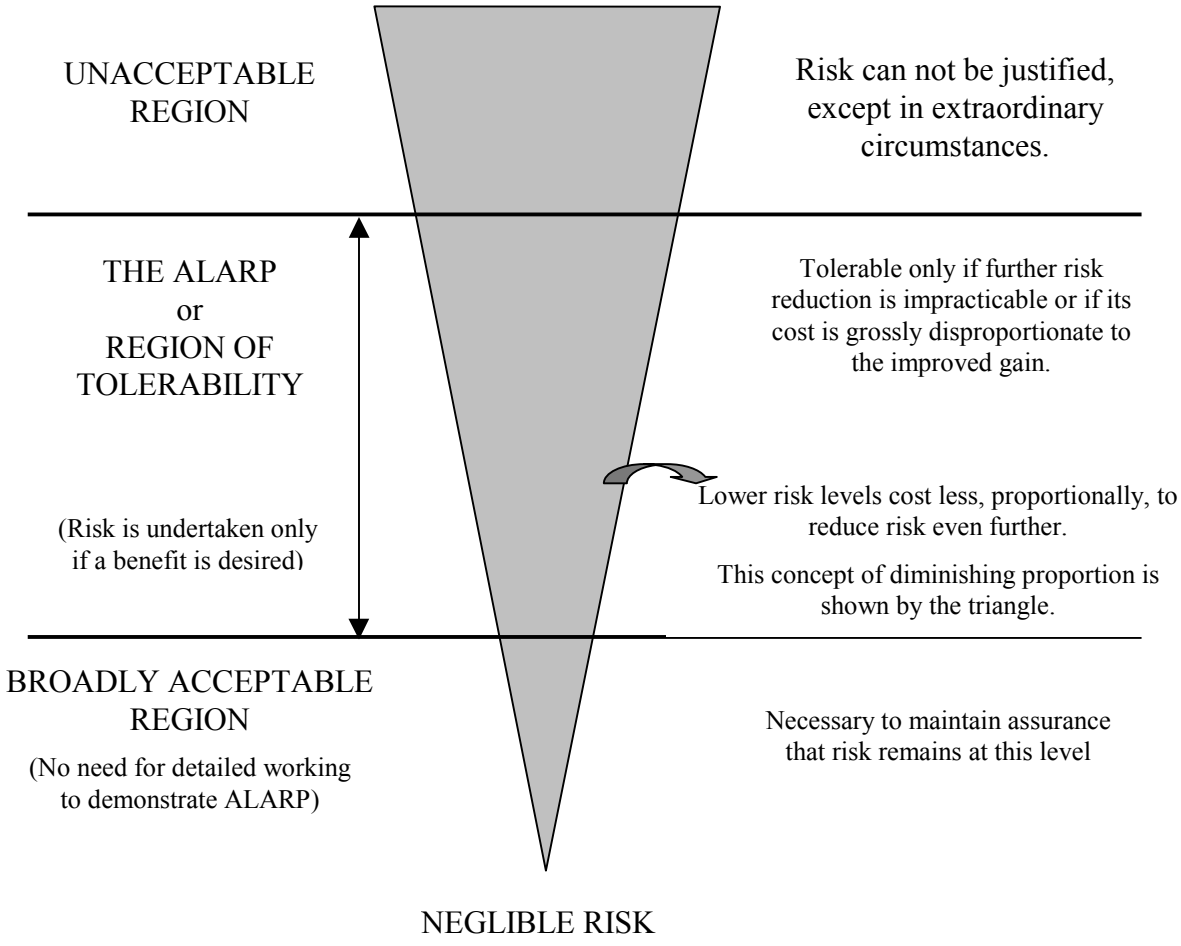
One system that is well worth considering is ALARP (As Low As Reasonably Practical). This is fully described in IEC 61508 part 5 [9]. Basically it divides the levels of risk into three regions:

a) Unacceptable (the risk is so great it must be refused altogether)

b) Broadly acceptable region (the risk is, or has been made, so small as to be insignificant)

c) ALARP or tolerability region (the risk falls between the two states specified above)

FIGURE 2 Levels of risk and ALARP



13.6 Hazard Log

Having identified the hazards, and determined the risks and the actions necessary to mitigate the risks, it then becomes necessary to record these facts.

This record becomes the hazard log. This should include all potential hazards, *even those considered as being too low a risk to worry about*. This is necessary so that the impact of design changes and requirements can be assessed.

This log is a living document and should be used continuously throughout the product/system lifecycle to provide traceability of the safety management process and evidence of the safety characteristics of the system.

The Hazard Log is also useful in court cases to help prove due diligence.

The Hazard Log should:

a) Identify the product & range of variants

b) Record all hazard identification and risk assessment details, together with the basis of assessment

c) Record risk control requirements, and trace their implementation, verification and validation

d) Record periodic reviews of the above and any necessary action

e) Record any reported accidents

f) Be managed in an organised way so that it can be used as legal evidence

g) Be a continuing archive (a live document)

13.7 Hazard Review

The hazards should be continuously reviewed.

A good practical way of ensuring that they are reviewed regularly is to include the Hazard review as part of the hardware and software design reviews. Hazards should also be reviewed at intervals outside these forums especially if design or requirement changes take place.

13.8 Safety Case

The safety case itself is the final report tying together all aspects of the safety process.

The safety case, which should be started as early as possible in a project's lifecycle, should contain the following information:

a) System description

b) Hazards

c) Prevention

In a full, formal safety case requirement this document may need to be audited by an independent assessor/consultant.

13.8.1 System Description

Information about the system, its subsystems, and equipments, describing their interfaces and functions.

This information can be drawn from many sources, e.g. design documentation, user manuals, operating instructions or handbooks.

13.8.2 Hazards

All the information used in the preceding paragraphs make up this section.

This should include reasoned arguments, assumptions made, and sources of information/evidence to support the arguments. There must be sufficient information present so that others can draw the same conclusion or challenge the results, if considered necessary.

13.8.3 Prevention

A description of the means employed to prevent the identified hazards from causing accidents.

14. Competency issues

14.1 Competency requirements for personnel involved in safety-related activities

All persons dealing with safety-related systems (including purchasers, operators, maintainers as well as designers and implementers) should be competent to perform their assigned tasks. Competence requires the qualifications, experience, and qualities appropriate to the duties. These include:

- Such training as would ensure acquisition of the necessary knowledge of the field for the tasks which they are required to perform
- Adequate knowledge of the hazards and failures of the equipment for which they are responsible
- Knowledge and understanding of the working practices of the organisations they work for
- The ability to communicate effectively with their peers, with any staff working under their supervision, and with their supervisors
- An appreciation of their own limitations and constraints – whether of knowledge, experience, facilities, resources, etc. – and a willingness to point these out

Professionals with responsibility for design, or for the supervision of personnel involved with safety-related activities, may in addition be expected to have:

- A detailed working knowledge of all statutory provisions, approved codes of practice, other codes of practice, guidance material and other information relevant to their work; an awareness of legislation and practices, other than these, which might affect their work; and a general knowledge of working practices in other establishments of a similar type
- An awareness of current developments in the field in which they work

Specific competencies are of four types:

- Technical skills; for example hazard analysis, report writing, etc.
- Behavioural skills; for example personal integrity, problem solving, attention to detail, etc.
- Underpinning knowledge; for example, a person performing a hazard identification must have knowledge of the particular application to be able to identify the likely hazards that exist
- Underpinning understanding; for example, it is unlikely that somebody could establish risk tolerability levels for a particular problem without an understanding of the basic principles of safety and risk

Safety-related professionals should be assessed against the competency requirements for a function and (if successful) credited with the competency to contribute to that function at one of three levels:

1) Supervised practitioner
2) Practitioner
3) Expert

The text above is taken from the IEE's '*Safety, Competency, and Commitment – Competency Guidelines for Safety-Related System Practitioners*' [15], with some small modifications to adapt it for use here. [15] was published in February 2000 as the result of a collaboration between the IEE and the British Computer Society, with the support of the Health and Safety Executive.

Annex B of [2] also contains useful guidance on the "Competency of persons".

14.2 Specific competency requirements for personnel involved in EMC-related safety activities

Persons who are competent to perform EMC compliance activities may *not* be competent to perform EMC-related functional safety activities. Persons who are competent to perform safety compliance activities may *not* be competent to perform EMC-related functional safety activities. It is important to ensure that personnel with different competencies interact in an effective way.

One of the difficulties with EMC-related functional safety is that it necessary to exercise a great deal of expertise and judgement in defining the reasonably foreseeable EM environment for safety-related systems. Estimating the risks associated with EMC-related functional safety issues is always difficult. As far as is known to the writers of this report at the time of its writing, no statistical rules or even broad guidelines have yet been published.

Personnel required to cross-over or bridge between the two disciplines of EMC and safety require appropriate competence and experience in real-life EM disturbances, electronic and software design, and functional safety. They especially need to have an understanding of the potential for low-probability EM disturbances in operational environments, such as:

- Close proximity to mobile and fixed radio, radar, and TV transmitters (including military, unlicensed, and illegal transmitters) and the reflections of their RF fields. The effects of mobile radiocommunications used by operators and others nearby are especially important.
- Natural and atmospheric disturbances (such as lightning and electro-static discharge).
- Disturbances caused by reasonably foreseeable electrical or electronic faults (such as device failure, marginal stability and self-oscillation, insulation failures, flash-over, earth-faults, fuse-blowing, circuit breaker operation).
- Disturbances caused by reasonably foreseeable human errors or misuse.
- Proximity of radio-energy equipment such as that covered by EN 55011 (especially Group 2).
- Disturbances caused by heavy power use, overhead transmission, HV switchgear, etc.
- Disturbances which can occur in the AC or DC power supplies powering the equipment.
- Lightning, including the ability to perform risk analyses to BS6651 Annex C (or EN 61312) and the ability to employ its installation design and construction requirements.

In addition, the requirements for these personnel include:

- In-depth understanding of the internal functioning of electrical, electronic, and programmable electronic apparatus and how these can be influenced by EM disturbances.
- In-depth understanding of the safety functions that the electrical, electronic, and programmable electronic apparatus perform in the applications concerned, and the implications of any failures.
- A clear understanding of what is involved in providing users and third parties with products, systems, and installations that achieve the levels of safety that they have a right to expect under present laws.
- The means and resources to keep their competency, knowledge, and understanding of all the above fields up to date at the levels required.
- The authority and resources which are at least adequate to ensure that, at the level required, what should be done to ensure EMC-related functional safety, is done.

15. Professional Conduct

The following rules of conduct summarise the IEE's requirements of its members working in the field of EMC and functional safety [16].

These rules set out an ethical standard of conduct that would be equally appropriate to other professionals and managers [17].

1) A member shall at all times take all reasonable care to ensure that his work and the products of his work constitute no avoidable danger of death or injury or ill health to any person.
2) A member shall take all reasonable steps to avoid waste of natural resources, damage to the environment, and wasteful damage to or destruction of the products of human skill and industry.
3) A member shall take all reasonable steps to maintain and develop his professional competence by attention to new developments in science and engineering relevant to his field of professional activity and shall encourage persons working under his supervision to do so.
4) A member shall not undertake responsibility as an electrical engineer which he does not believe himself competent to discharge.
5) A member shall accept personal responsibility for all work done by him or under his supervision or direction, and shall take all reasonable steps to ensure that persons working under his authority are competent to carry out the tasks assigned to them and that they accept personal responsibility for work done under the authority delegated to them.
6) A member called upon to give an opinion in his professional capacity shall, to the best of his ability, give an opinion that is objective and reliable.
7) A member whose professional advice is not accepted shall take all reasonable steps to ensure that the person overruling or neglecting his advice is aware of any danger which the member believes may result from such overruling or neglect.

16. References

[1] *Safety-related systems*, IEE Professional Brief

[2] IEC 61508-1:1998 *Functional safety of electrical / electronic / programmable electronic safety-related systems* - Part 1: *General Requirements*

[3] IEC 61508-2 *Functional safety of electrical / electronic / programmable electronic safety-related systems* - Part 2: *Requirements for electrical / electronic / programmable electronic safety-related systems*

[4] IEC 61000-2-5 *Classification of electromagnetic environments*

[5] *EMC Directive* 89/336/EEC as amended. UK implementation: S.I. 1992/2372 *The Electromagnetic Compatibility Regulations 1992* amended by S.I. 1994/3080, S.I. 1995/3180

[6] IEC 61000-1-1 *EMC - Application and interpretation of fundamental definitions and terms*

[7] IEC 61508-6 *Functional safety of electrical / electronic / programmable electronic safety-related systems* - Part 6: *Guidelines on the application of parts 2 & 3* (still in preparation)

[8] Draft IEC 61000-1-2 EMC - Part 1, General - Section 2*: Methodology for the achievement of functional safety of electrical & electronic equipment* (the latest draft at the time of writing (March 2000) is IEC CDV 77/61000-1-2 Ed.1)

[9] IEC 61508-5 *Functional safety of electrical / electronic / programmable electronic safety-related systems* - Part 5: *Examples of methods for the determination of safety integrity levels*

[10] BS 4778 Quality Vocabulary: Part 3 *Availability, reliability and maintainability terms* Section 3.1:1991 *Guide to concepts and related definitions*

[11] ISO/TMB draft standard N12 on *Risk Management Terminology*

[12] *Machinery Safety Directive* 89/392/EC. Implemented in the UK by S.I.1992/3073 *The Supply of Machinery (Safety) Regulations* and amended by S.I. 1994/2063. Since replaced by the consolidated edition 98/37/EC.

[13] Council Directive 85/374/EEC of 25 July 1985 on the *Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products* [OJ 1985, L 210/29]

[14] *Low Voltage Directive* 73/23/EEC amended by 93/68/EEC the *CE Marking Directive*. Implemented in the UK by S.I.1989/728 *The Low Voltage Equipment (Safety) Regulations 1989,* and amended by S.I. 1994/3260 *The Electrical Equipment (Safety) Regulations 1994*

[14bis] *Radio & Telecommunications Terminal Equipment Directive* 99/5/EC. Implemented in the UK by S.I. 2000/730 *The Radio Equipment and Telecommunications Terminal Equipment Regulations 2000.*

[15] *Safety, Competency, and Commitment – Competency Guidelines for Safety-Related System Practitioners* 180pp ISBN 0 85296 787 X, available from IEE Publications Ref: PA 023

[16] IEE Professional Brief *Professional Conduct, 1992*

[17] The Engineering Council's *Guidelines on Risk Issues, 1993*

[19] *Report of the SLIM III Team on the Electromagnetic Compatibility Directive (89/336/EEC as amended)* Final version, Brussels, 24th September 1998

Amended 04.01.01

[20] *Considerations on Safety and EMC*, pages 6 and 7 of EMC-consultant / commission 6 12/05/99 Annex A to CLC(SG)765, C210(Sec)151. A statement by Mr R De Vré (EMC consultant to the European Commission) tabled at the CENEEC/ETSI ad hoc meeting held on 18th May 1999 in Brussels.

17. Bibliography and further reading

The following may provide additional information and guidance:

EMC for Systems and Installations, T. Williams and K. Armstrong, Newnes, December 1999, ISBN 0 7506 4167 3

IEC 61508 Principles and Use in the Management of Safety, Felix Redmill, IEE Computing and Control Engineering Journal, October 1998 pp 205-214

Product Safety, C Hodges, M Tyler, and H Abbott, Sweet and Maxwell, London, 1996, ISBN 0 421 50370 X

Dangers of Interference – EMC and Safety, Simon Brown, Health and Safety Executive, EMC Supplement to the IEE's Electronics Communications and Control Journal, July 1994, pp S-11 to S-13.

Safety and Reliability – key facets of EMC for installations, Tony Maddocks, Manager EMC Division, ERA Technology, Approval magazine Jan/Feb 1997 pp 29-31.

EMC Management for Hazardous Installations, a workshop held at the IEE's 10th International Conference on EMC, University of Warwick, 1st September 1997. The workshop papers are available from the IEE's Conference Executive, phone: 0207 344 5467.

Amended 04.01.01

18. Glossary of terms used in this report

These descriptions are provided as an aid to understanding. Formal definitions may be found in the IEC International Electrotechnical Vocabulary. Words in *italics* are described elsewhere in this glossary.

Brownout	USA term for a dip: a reduction of the supply voltage well below its normal tolerances, followed by a recovery to the original level. The voltage during the dip does not reduce to zero. Brownouts can last for seconds, minutes, or even hours.
Common cause failure (CCF)	A failure which is the result of one or more events, causing coincident failures of two or more separate channels in a multi-channel (redundant) system, leading to the defined system failing to perform its intended function.
Common-mode voltage	A voltage that applies identically to all the conductors (including return conductors and shields) associated with a cable, or with an item of equipment.
Conducted (emissions, transients)	Unwanted energy conducted from equipment via the power supply or signal cables.
Continuous disturbance	A *disturbance* which cannot be resolved into a succession of distinct events by measuring equipment, typically applied to disturbances which occur more than 30 times a minute on average.
Disturbance	Unwanted EM energy, which may or may not cause a problem to victim equipment. Disturbances may be produced by either intentional or spurious sources, from equipment, or by natural causes (e.g. lightning, or *electrostatic discharge*).
Dropout	A sudden reduction of the mains supply voltage to zero for short period of time, followed by a recovery to the original level.
EM	Electromagnetic
Electromagnetic Compatibility (EMC)	The ability of equipment or a system to function satisfactorily in its *electromagnetic environment:* - without introducing intolerable electromagnetic *disturbances* into that environment, and: - without suffering unacceptable degradation of performance due to the electromagnetic *disturbances* present in its environment.
Electromagnetic interference (EMI)	The result of inadequate immunity to *disturbances*.
Electromagnetic environment	The totality of the electric, magnetic, and electromagnetic fields, conducted energy, and electrostatic fields and discharges in a particular location.

Electrostatic discharge	Otherwise ESD. A sudden transfer of electric charge from one body to another, usually because of the voltage breakdown of the air between them (a spark). The dissipation of the charge causes *transient* disturbing currents to flow, and the spark is a source of very wideband *radiated emissions*.
EMC	See *Electromagnetic compatibility* above
Fast transient	Usually used to describe an impulse with a risetime of around 5ns on power or signal cables. Most likely to appear in the form of a *burst* of such *transients*.
Filter	A combination of capacitors, inductors and/or resistors to prevent electromagnetic energy at unwanted frequencies from being conducted along a cable or wire.
Flicker	Rapid fluctuations in the mains supply voltage, perceivable by the eye as a flickering in the illumination provided by electric lamps and luminaires.
Functional safety	That part of the overall safety which depends on the correct functioning of electrical / electronic / programmable electronic equipment or systems.
Grounding	In EMC terms, the interconnection of reference circuits to present a low impedance reference for signal or filtering circuits, and so minimise noise. It may or may nor be at the potential of the earth mass, and is not necessarily the same as the safety earth or protective conductor.
Harmonics	Frequencies which are a multiple of the fundamental sine wave. On mains supplies they are caused by the power supplies of equipment drawing current in a non-sinusoidal manner, which distorts the waveform.
Interference	The result of inadequate immunity to *disturbances*.
Inter-harmonics	Frequency components which are not an integer multiple of the fundamental frequency.
Nuclear EM pulse (NEMP)	An extremely high intensity pulsed field caused by the gamma rays emitted in an exo-atmospheric nuclear explosion. Field strengths of 50kV/m are possible.
Radiated emissions	Energy transmitted as EM waves.
Safety-critical	Where correct operation is necessary for the prevention of safety hazards or risks.
Safety integrity level (SIL)	(From IEC 61508 part 4) A discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the electrical / electronic / programmable electronic safety-related equipment or systems. SIL 4 has the highest level of safety integrity, and SIL1 the lowest.

Screening	An alternative term for *shielding*, often applied to the conductive covering of shielded cables.
Shielding	The use of conducting material to form a barrier to EM waves, so that they are reflected or absorbed.
Spike	An alternative term for *transient*.
Surge	A form of *transient,* which has a higher energy content, typically produced by the current from a lightning strike coupling into long cables such as power supply or telecommunication cables. A surge has much longer risetimes and decay times associated with it than fast transients.
Technical Construction File (TCF)	A document created by a manufacturer to set out his argument as to why his product or system meets the protection requirements of the EMC Directive. Employed in one of the three routes to compliance set out in the EMC Directive, and always requiring assessment by an appointed EMC Competent Body.
Transient	A rapid change of the waveshape of voltage, current, or field, of very short duration followed by a return to steady state.
Varistor	A voltage-dependant resistor commonly used to limit voltage transients.

19. Contributors to this guidance document

19.1 Members of the IEE Working Group

A list of the members of the IEE Working Group on EMC and Functional Safety from September 1998 to February 2000:

Eur Ing Keith Armstrong	Partner, Cherry Clough Consultants (chair of this WG)
Peter Burt	Technical Consultant (Safety), ERA Technology Ltd
Eur Ing Simon Brown	HM Principal Specialist Inspector (Control and Instrumentation), Health and Safety Executive
Vic Clements	Senior Consultant, Radio Frequency Investigations Ltd
Dai Davis	Head of IT, Communications, and New Media Group Nabarro Nathanson
John Davies	EMC Manager, Celestica plc
Roger Emberson	Technical Head of Telecommunications, Kvaerner Oil and Gas Ltd
Dr Alwyn Finney	EMC Manager, ERA Technology Ltd
Ray Garner	EMC Consultant, Datel Defence Ltd
Dr Bob Holmes	Engineering Consultant, Green Leader Ltd (previously with W S Atkins Rail Ltd)
Peter Kerry	Manager (EMC and Research), Radiocommunications Agency and President of CISPR
Richard Marshall	Director, Richard Marshall Ltd
Les McCormack	Principal EMC Engineer, York EMC Services Ltd
Mr Ian MacDiarmid	Consultant in Electromagnetics, British Aerospace Military Aircraft
Mr Anthony McLaughlin	Type Approval Department, Lloyds Register of Shipping
Dr Ian Noble	Engineering Consultant
Dr David Ward	Head of Research – Electrical Group, MIRA (Motor Industry Research Association)
Mr John Whaley	General Manager, International Electrical Approvals, SGS UK Ltd

19.2 Other contributors

Some of the material in this report was also provided by the following: Derek Fowler of CSE International; George McDowell, Elaine Greig, David Atkey, and Oona Nanka-Bruce of ERA Technology Ltd; Terry Smith, Ron Watson, and John Wright of Corus (British Steel).

A number of other people also assisted with reviewing and commenting usefully on the various drafts of the core document and its industry annexes, including colleagues and associates of the above, and the chairman (Professor Andy McGettrick) and members of the IEE's Safety Critical Systems Committee.