Another EMC resource
from EMC Standards

EMC-Related Functional Safety of Electronically Controlled Equipment

Helping you solve your EMC problems

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

EMC-Related Functional Safety of Electronically Controlled Equipment

Keith Armstrong

More than meeting regulatory immunity requirements—where such exist—it is necessary to ensure user safety when devices are subjected to electromagnetic disturbances.

As seemingly everything comes to be controlled by electronics, the immunity of electronic equipment to foreseeable electromagnetic (EM) disturbances becomes more important for satisfying safety and product liability laws. EM disturbances can have serious consequences for product functional safety, even where all of the immunity requirements of the EMC Directive or other applicable directives or regulations have been fully complied with.

Replacing the old electromechanical energy regulators of such appliances as the domestic deep fryer or electric blanket with electronic controls can add functionality for little cost. However, some appliance manufacturers may be too new to the electronic technologies world to realize that power-line transients or a nearby cellular telephone could cause the heat output of their products to increase to dangerous levels, leading to burns, fires, or death or injury from hyperthermia. Such scenarios involving domestic appliances, even ones having potentially fatal consequences, although not often made public, have happened.

So, as electronic controls, particularly programmable devices, find their way into just about everything, they are too often being incorporated into products by designers with little experience of relevant safety and electromagnetic compatibility (EMC) issues. Indeed, some manufacturers may not even think that the concept of safety is related to the electronic devices in their equipment products, nor would they know what to do about it if they did.

Industrial robots and machinery normally are controlled by low-cost programmable devices. Great care is taken by their manufacturers to install guarding and other mechanical and electrical safety measures. And if the products are to be sold in the European Union (EU), the manufacturers might do some emissions and immunity testing to meet the minimum levels set by the EMC Directive. But manufacturers usually only guard the programmed movement range: They may not have thought about the human safety implications of the robot arm or machine making an uncommanded maneuver, moving beyond its

programmed settings, or altering its speed or torque settings (during "teach" or maintenance modes, for example). Such program corruption is a typical result of inadequate immunity to local EM disturbances. The potential for such dangerous occurrences must be assessed fully and dealt with for reasons of safety, not because EMC regulations say something about it.

The implications that foreseeable EM disturbances can have for functional safety in the brave new coming world of drive-by-wire and the like could mean that even transportation industry professionals, whose understanding of safety and EMC issues is generally good, will face a few EMC-related surprises. In fact, few safety experts are knowledgeable about the kinds of real-life EM disturbances that products might foreseeably be exposed to, or how those products' electronics might respond to such threats. Few EMC experts, for their part, are accustomed to the language and disciplines of safety, or are comfortable dealing with hazards and risk analyses, and related statistical and probability issues. That a product has passed a regulatory EMC test tells the EMC specialist nothing about whether it may harbor significant EMC-related safety problems.

EMC and safety engineers working for manufacturers thus may know everything they need to know to make products meet the standards required by regulatory authorities, while at the same time having insufficient knowledge or experience of the possibility of EMC-related safety incidents occurring in the real world to be able to mount a strong defense against certain types of product liability claims. And this is not just about immunity. Product emissions within regulatory limits can also be a cause of functional safety problems in nearby equipment, as the medical device industry well knows.

Safety standards and laws very rarely acknowledge EM disturbances or EMC, and only now are most of the safety standards writers at the International Electrotechnical Commission (IEC) and in the EU starting to think about these issues. The Machinery Safety Directive and some of its standards do mention EM disturbances, but they do not cover the relevant issues clearly or comprehensively. As a result, some machinery notified bodies in the EU give conflicting advice on this issue.

IEC 61000-1-2 on EMC and Functional Safety is expected to be published during 2001, but only as an IEC technical report and not as a standard.[1] The new standard on functional safety, IEC 61508, is a rare example of a safety standard that correctly describes how EM disturbances should be treated as possible causes of error or malfunction.[2] But it is not (yet) an EN. It is even less likely to ever become harmonized under any EU directives.

In the EU, and probably in many other trade areas and countries, mere compliance with a safety standard may not be sufficient legal defense that the product was, in fact, safe enough. This is why, for example, the Machinery Directive requires performance of a hazards and risk analysis that must consider every "foreseeable" circumstance.

The British Institution of Electrical Engineers (IEE), headquartered in

London, feared that, in light of the foregoing, many unanticipated safety problems could be in the offing.[3,4] In 1998, IEE set up a working group to produce a professional guidance document for managers and engineers. The group included renowned EMC and safety experts from a wide range of industries and senior officers from Britain's regulatory Health and Safety Executive.

The IEE guide on EMC and functional safety was published in September 2000.[5] IEE believes the guide to be the first published on this subject. It describes how to control EMC when functional safety issues are involved and is intended for use by both engineers and their managers.

The guide consists of a core section that discusses the central issues, and eight industry annexes, each showing how a particular industry has addressed, or should address, EMC-related functional safety, and each written by an expert working in that industry. Another annex, on software and EMC-related safety, will be especially valuable in the future as more and more safety-related functions are controlled by programmable electronics.

The core section includes an interesting set of brief descriptions of safety incidents in which lack of EMC was proved to be the cause. Because of the statistical nature of EM disturbances (see discussion below) and the unfamiliarity of most people with them, it is thought that many safety incidents characterized as "no fault found" were caused by interference.

The IEE publication can be downloaded in Word or PDF formats from http://www.iee.org.uk/PAB/EMC/core.htm (the URL is case sensitive).

This article, following the IEE guide, is written from the perspective of having to meet EU directives on safety and EMC. Like the new guidance document, it explains why meeting immunity standards may in itself be insufficient to ensure functional safety, and it describes what responsible professionals should do.

What Is Meant by EMC?

EMC is achieved when the EM disturbances emitted by a piece of equipment are low enough not to upset the operation of other equipment and when an equipment piece has sufficient immunity to EM disturbances in its environment to function adequately. EM disturbances include power-supply voltage dips, dropouts, brownouts, and waveform distortion; voltage surges on power lines and long cables; fast transients; electric and magnetic fields; and radio-frequency (RF) fields and induced currents up to many gigahertz.

Inadequate EMC can allow a received radio signal to be confused by competing signals and noise, causing what is known as *interference*. Interference can hamper or prevent the function of an electronic device, which can in turn sometimes put operators, patients, or other users at safety risk.

EMC as the condition of maintaining freedom from interference in the

operation of electronic equipment is increasingly important because of several trends in technology.

- Mobile radio transmitters such as cell phones and walkie-talkies intentionally create powerful RF fields within a meter or so of their antennas and are becoming ubiquitous.
- Modern electronics technologies such as digital and switched-mode generate more EM disturbances as an inevitable side effect of their design and operation modes.
- Semiconductor chips, or integrated circuits, have smaller physical features and supply voltages and, as a direct consequence of this, are more likely to suffer malfunction or damage due to EM disturbances.
- Electronics will soon be used to control almost every instrument and appliance with the potential to be so controlled.

What Is Meant by Safety?

Safety is the term used to denote the concept of a consensual understanding of the hazards, and their risks, that are acceptable to a given society. For example, people accept hazards up to and including the death of entire families when traveling by road, as long as the risk of these hazards occurring is low enough. They accept greater hazards and risks for adults than for children, and they understand that some types of activities carry greater hazards or risks than others. Safety laws generally require products to be designed and manufactured so as to be as safe as people "have the right to expect."

Functional safety is the term used to cover the hazards and risks associated with errors or malfunctions in the intended functionality of a device or an apparatus. This is distinct from *intrinsic safety*, which designates a device's potential for causing such hazards as fire, cutting, electric shock, and toxic fumes.

Designers of safety-related systems are expected to create documented safety arguments. These should include hazards and risks analyses that take account of at least the following eventualities:

- Reasonably foreseeable misuse of the design, whether accidental (such as incorrect installation or human error) or deliberate (such as overload or use for an unintended purpose).
- Reasonably foreseeable faults in the design, especially component failures.
- Reasonably foreseeable environmental extremes, including, among others, high temperatures, condensation, exposure to EM disturbances, and vibration.
- Reasonably foreseeable consequences (hazards), with their probabilities (risks), of the foregoing eventualities.

The safety argument also should include an analysis of whether the design achieves the safety that people "have the right to expect" at the time and, if not, what needs to be done to achieve this.

The Relationship of EMC and Functional Safety

Whenever an electronic device controls an appliance or system that, if it went wrong, could put the operator or third parties at a higher risk, then the accuracy and reliability of the controlling electronics becomes a safety issue. But all types of electronics are susceptible to inaccuracy, malfunction, or damage due to EM disturbances; consequently, safety hazards or risks can be exacerbated by the absence of adequate EMC.

Many engineers and their managers believe that any equipment declared by its manufacturer to be in conformity with the EMC Directive must be free from all EMC problems. But the directive is concerned solely with removing technical barriers to trade within the EU single market and cannot, by its limited nature, properly deal with EMC-related functional safety issues.[6] It takes into account only normal operation and typical EM environments (see Figure 1). By contrast, safety compliance in the EU involves mandatory consideration of reasonably foreseeable low-probability events, human error and misuse, operational overload and environmental extremes, and faults in the apparatus itself and other nearby equipment. Also, the scopes of the EMC Directive's immunity standards specifically exclude safety considerations.

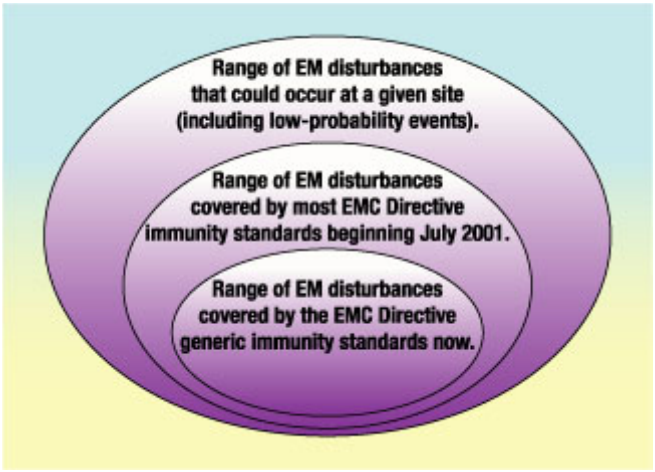

Figure 1. Schematic approximation of the extent of possible EM disturbances to which electronic equipment could be susceptible by comparison with the coverage range of present and future immunity standards.

Current safety legislation requires manufacturers to take a safety argument approach to all EMC issues that could possibly have an adverse effect on safety by increasing hazards or risks (sometimes called a safety case). This includes EU directives covering low-voltage equipment, machinery, medical devices, gas appliances, construction products, personal protective equipment, product liability, general product safety, toy safety, and health and safety at work.

The UK also has safety regulations applicable to plant or large engineering projects that implicitly require EMC performance to be addressed from a functional safety perspective. Examples are the Provision and Use of Work Equipment Regulations (1998); Offshore Installations (Safety Case) Regulations as amended by the Offshore Installations and Wells (Design and Construction, etc.) Regulations (1996); Offshore Installations (Prevention of Fire and Explosion, and

Emergency Response) Regulations (1995); and Control of Major Accident Hazard Regulations (1999). Most other developed nations have similar safety legislation covering the safety of large engineering projects.

Most transportation industries have traditionally treated EMC as a safety-related issue, often out of fear of liability claims. But even some safety experts in these industries have expressed concerns about the EMC approach being taken, partly in response to the rapidly increasing number of safety-related functions being controlled by electronics, such as drive-by-wire.

How should EMC be controlled to achieve functional safety? The IEE guide recommends, in essence, answering that question by first pursuing the following questions to the answers they may yield:

- What EM threats could the equipment be exposed to?
- What could happen as a result of these EM threats?
- How might the equipment's EM emissions affect other equipment?
- What could be the reasonably foreseeable functional safety implications?
- What actions are needed to achieve the required safety level?
- What documentation is required to show that safety has been achieved?

The economic argument for heeding the advice offered by the guide comes from a much earlier stage of industrial history: A stitch in time saves nine. The money saved on 999 projects by cutting corners on EMC-related safety can easily be lost by just one safety incident attributable to the thousandth. In addition, a single safety incident can lose a company its long-established reputation overnight. Designers do not always take into account the possible consequential costs to their employers of getting the safety design wrong. As a result, some companies may be running much greater financial risks than they know.

This article now looks at the fundamental questions just itemized in some detail.

Exposure to EM Disturbances

What EM threats could the equipment be exposed to?

To answer this question properly requires an assessment of all the EM disturbances the equipment could possibly be exposed to, however infrequently, in its foreseeable operational environment. IEC 61000-2-5, IEC 61000-2-6, and lightning standards such as BS 6651 Annex C, IEC 61312-1, or IEEE C62.21, among other standards, can help here; but many documents pertaining to the EM environment consider only typical exposure to EM disturbances and do not address the statistical distribution of all possible threats. It is only when the statistical likelihood of a threat is expressed quantitatively that safety risks of the event possibility can begin to be assessed.

Measurements can confirm the levels of some EM threats, but they can

only indicate their present state. The readings may not be able to suggest the full range of possibilities of the disturbance sources.

A good example of an increasingly common EMC problem is the bringing of such mobile radio transmitters as walkie-talkies (private mobile radio), cell phones, and vehicular mobile radios into proximity with electronic equipment. Although these transmitters are not very powerful, they can come near enough to the equipment to expose it to powerful RF fields—more powerful than those it was tested to for compliance with the immunity standards harmonized under the EMC Directive, for example.

The EMC Directive's immunity standards require manufacturers of most computer and light industrial equipment to declare that the equipment will function adequately in RF fields of up to 3 V/m. So how near do mobile radio transmitters have to be to exceed 3 V/m? Figures 2 through 4 illustrate some commonplace situations involving different levels of transmitting power.

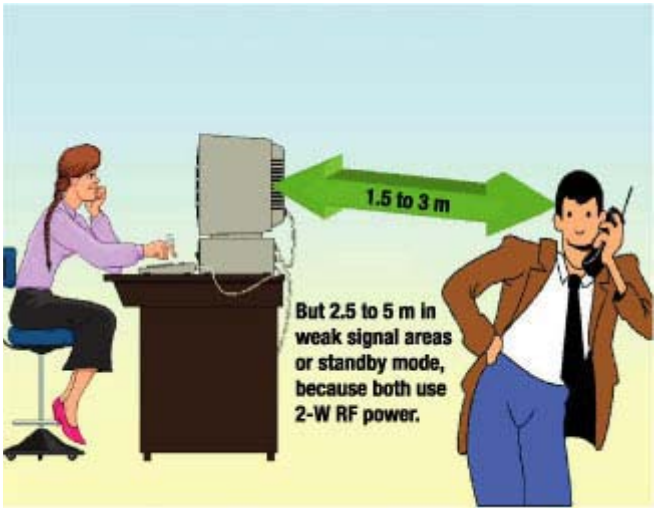

Figure 2. Distance within which a typical cell phone in a strong signal area (0.8-W RF power) creates an RF field of 3 V/m. Actual distance depends on whether metal objects or structures are nearby.

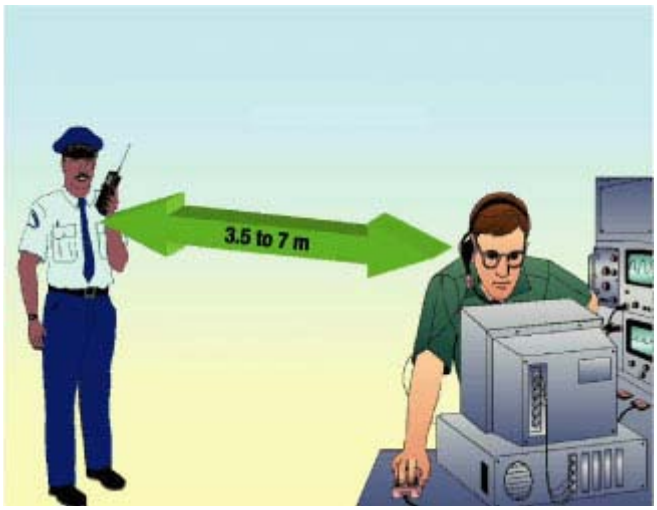

Figure 3. Distance within which a typical private mobile radio handset (walkie-talkie) with 4-W RF power creates an RF field of 3 V/m. Actual distance depends on how nearby metal structures and

objects are.

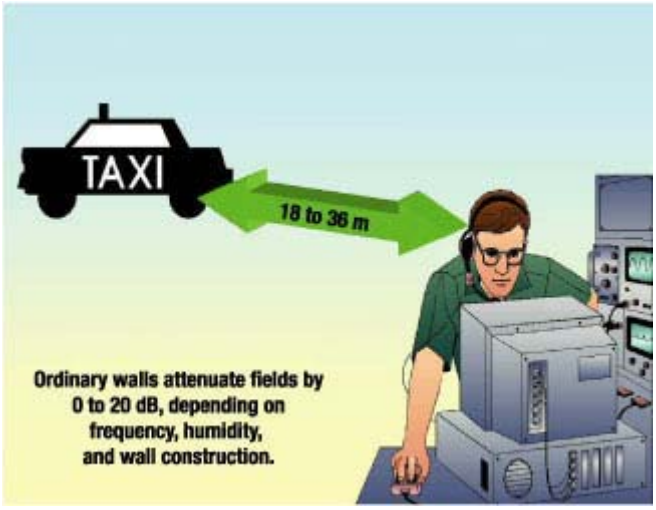

Figure 4. Distance within which a typical mobile VHF/UHF transmitter with 100-W RF power creates an RF field of 3 V/m. Actual distance depends on reflections from nearby metal objects and structures.

Manufacturers of computers and equipment for use in industrial plants are required by the EMC Directive to declare that these items will function adequately in RF fields up to 10 V/m. To calculate the range within which mobile transmitters can exceed these levels, divide the distances shown in Figures 2 through 4 by 3. Figures 2 and 3 suggest that people should not use cell phones or walkie-talkies if they are within several meters of an electronic apparatus unless the equipment has been designed and tested to be safe under such circumstances.

Large computer systems constructed from components that individually meet the 3-V/m limit are often found to achieve only 1 V/m as a system. Consequently, for such systems, the distances in the three figures should be multiplied by 3 to determine the proximity range of mobile radio-communication devices that could threaten errors or failures. A similar degrading of immunity performance can occur with any complex system, even where it has been carefully installed by knowledgeable people.

The handheld transmitter provides just one example of how compliance with the EMC Directive may not be enough to eliminate EMC-related functional safety issues. EM threats come from many other sources. For instance, RF fields with frequencies or amplitudes that can easily be higher than those covered by the directive's immunity standards are generated by microwave ovens and dryers; wireless local-area networks and other microwave communications; industrial, scientific, and medical equipment using RF energy for its primary function; mobile-communications base stations; radio and television broadcast stations; vehicle-mobile transmitters; and radars.

Only starting in July 2001 will most equipment sold in the EU have to be declared as withstanding a limited range of surges typical of the effects of lightning on utility power distribution. Surges can cause

physical damage to electronics; thus, restarting the equipment may not do any good, and software solutions to interference problems, such as data protocols, may have limited effectiveness. Lightning is an example of an EM disturbance that can only be considered statistically. Various organizations record lightning activity and publish contour maps showing strike density per unit of area, but these are not exactly planning tools. Lightning activity can vary fourfold from year to year, and strike intensity itself is subject to wide variation.

Dips and dropouts in the main power supply are a significant problem that some large plants have spent tens of millions of dollars to try to overcome. Another power-line quality problem that can affect equipment is the increase in harmonic currents (causing waveform distortion) that can lead to overheating in cables, motors, and transformers, with obvious safety implications.

Consequences of Exposure

What could happen as a result of EM disturbances?

What is important is to consider all the reasonably foreseeable consequences of exposure to the threats identified in investigating the previous question. Disturbances can cause physical-parameter measurements to suffer errors of as much as plus or minus full-scale deflection. Such an effect is bad news for such critical concerns as crane safe-load indicators; control of exothermic reactions; control of vehicle speed, braking, direction, and so on; and control of flow, temperature, pressure, and other physical variables.

In addition, programmable equipment and systems can suffer from any number of malfunctions. False key-presses can be registered, errors in reading external transducers can indicate that a shut door is open or vice versa, a robot or machine can undergo a change in operational mode without receiving a true command, and software can operate incorrectly, for example, continually repeating an inappropriate subroutine. And of course, total failure—that is, a crash—can occur, leaving control outputs in any possible combination of states, including ones in which it may be physically impossible to achieve in reality—possibly causing new types of safety hazards.

Effects of Equipment Emissions

How might the equipment's EM emissions affect other equipment?

Harmonized EMC emissions standards warn that they do not cover situations "where sensitive equipment is used in proximity," but without specifying what they mean by "sensitive" or "proximity." Most of these standards are also limited in coverage to frequencies below 1 GHz. However, modern computers can easily have significant emissions at 2 GHz and higher, and some types of equipment are allowed to produce unlimited emissions levels at specified frequencies.

Interference with radiotelephones and radio receivers is not uncommon, because these instruments are very sensitive, but even plain old

telephones become safety critical when there is a need to phone emergency services. For example, there is a well-documented instance of power converters in a North Sea Gas pumping station in Scotland making ordinary telephones as far as 20 miles away unusable.

Risk to Functional Safety

What functional safety implications might be reasonably foreseen?

This analysis should take into account the severity of any possible safety hazard and the scale of the risk. It could employ a safety integrity level (SIL) specification along the lines presented in IEC 61508.[2]

Safety Responses

What actions need be taken to achieve the required level of safety?

Safety and reliability engineers are used to electronic faults appearing randomly. Burn-in techniques and duplicated or triplicated systems are often employed to improve reliability, with the replicated systems commonly using identical components and cable routing. But electromagnetic interference creates common-cause faults; that is, similar components, circuits, equipment, or systems can fail in exactly the same way, at the same time. Consequently, when replicating critical functions, it is important to use different technologies and to run any replicated cables via different routes.

Thought must also be given to the diversity and reliability of power supplies. Even uninterruptible power supply equipment may be no more reliable than the utility power it is supposed to improve upon—such cases are known—so battery backup ought to be carefully considered.

EMC proof testing of the final design is an obvious step, but if equipment is designed poorly for EMC, then the results of such tests are meaningless in serial manufacture. Or their significance may be dependent on the EMC skills of operating, maintenance, or repair staff. The necessary EMC performance for all safety-related areas thus should be designed in from the beginning of the design phase.

A natural desire to test all safety-related functions on every piece of equipment installed for their assessed EM threats is sometimes not feasible to satisfy. An EM incident could conceivably destroy large portions of equipment function, and yet this might be allowable as long as the equipment never becomes unsafe. Testing for this possibility on each item of installed equipment would never leave one undamaged.

Documentation of Assured Safety

What documentation is required?

Larger projects that require approval or certification by regulatory safety bodies should include EMC in their safety argument. The safety argument, or safety case, approach to considering EMC and functional safety is always recommended, although for some projects this may

involve quite a slender document. The Low Voltage and Machinery Directives both require documented safety arguments, which should also cover EMC-related functional safety possibilities.

Such documented safety arguments will be valuable in reducing exposure to product liability claims. Existing liability laws in the EU place the burden on manufacturers to prove that, on balance of probabilities, their equipment was not likely to have caused the damage, injury, or financial loss being claimed. Most developed countries have similar product liability laws.

Project records need to show that the appropriate EMC performance was determined and then designed in, for all safety-related areas, right from the project's start. Manuals and other documentation supplied to the user should include full information on all EMC aspects of installation, maintenance, operations, use limitations, and warnings. Limitations to use might involve such things as banning mobile phones within a certain area or taking required precautions to protect against effects of lightning. A recent cautionary example is a company found guilty of "failure to warn" that the semiconductor equipment it manufactured had a propensity to open all its valves and release chlorine gas into the workplace when subjected to quite normal levels of power-line voltage transients.

In sum, it is vital that manufacturers design any hazards or risks out of their equipment as far as that is possible, and that they not rely on guard devices or printed warnings or a presumption of operator skill to provide the safety that people "have the right to expect."

Conclusion

EMC-related functional safety is a complex, cross-disciplinary area of technical expertise whose practitioners need to be well versed in all matters pertaining to the electromagnetic environment. Too many EMC engineers and managers now are familiar only with regulatory or contractual EMC issues and know little about statistical distributions of typical and unusual EM threats. And for their part, safety engineers and managers often know very little about EMC.

Many professionals in both disciplines lack sufficient knowledge to assess all the possible effects of EM disturbances on electronic circuits and software and to calculate and interpret their statistical distributions. Clearly, electronic equipment manufacturers need to carefully recruit staff who have the necessary competencies and expertise to work on EMC and functional safety issues in tandem. Or they can achieve the same ends through training.

Maintenance and repair personnel are often overlooked in this regard. They are not usually EMC or functional safety experts; they may not see the importance of closing a cabinet door fully, replacing all the fixing screws in a panel and applying the correct torques, or reading and completely understanding the manufacturer's manuals before beginning any work. Where safety is an issue, competency is also an issue—for everyone involved with the equipment or system, over its whole

operational lifetime.

References

1. Electromagnetic Compatibility, Part 1: General, Section 2: "Methodology for the Achievement of Functional Safety of Electrical and Electronic Equipment with Regard to Electromagnetic Phenomena," Draft 77/231/CDV—the future IEC 61000-1-2 (Geneva: International Electrotechnical Commission, 1999).

2. "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems," IEC 61508 (Geneva: International Electrotechnical Commission).

3. Simon Brown, "Dangers of Interference—EMC and Safety," *IEE Review* (July 1994): S-11–S-13, special EMC supplement.

4. "EMC Management for Hazardous Installations," workshop presented at the Institution of Electrical Engineers 10th International Conference on Electromagnetic Compatibility, Warwick, UK, September 1–3, 1997.

5. Institution of Electrical Engineers, *IEE Guidance Document on EMC and Functional Safety* (London: IEE, 2000).

6. R de Vré, "Considerations on Safety and EMC," in Annex A to CLC (SG)765 C210(Sec)151, (December 5, 1999): 6–7, unpublished internal EC document.

Keith Armstrong is a founding partner of Cherry Clough Consultants. He can be reached at keith.armstrong@cherryclough.com

Back to 2001 Annual Reference Guide Table of Contents