Another EMC resource
from EMC Standards

The IET's Guide on EMC for Functional Safety

Helping you solve your EMC problems

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

The IET's Guide on EMC for Functional Safety

Keith Armstrong
www.cherryclough.com

Electronic complexity is increasing with no end in sight, increasing self-generated noise levels, whilst the feature sizes in silicon integrated circuits continue to shrink making them emit more noise whilst at the same time more susceptible to noise. The use of electronics in safety-related applications is growing very rapidly indeed, with (once again) no end in sight.

We have already reached the point where the normal testing-based approach to electromagnetic compatibility (EMC) is totally inadequate where safety is concerned, as current media interest in automobiles with malfunctioning "electronic throttles" shows.

The inevitable consequence of all these trends is that without a new approach to electromagnetic compatibility (EMC) engineering, there *will* be uncontrolled safety risks for people in general, plus uncontrolled financial risks for manufacturers and service providers who employ electronic technologies, as Figure 1 attempts to show.

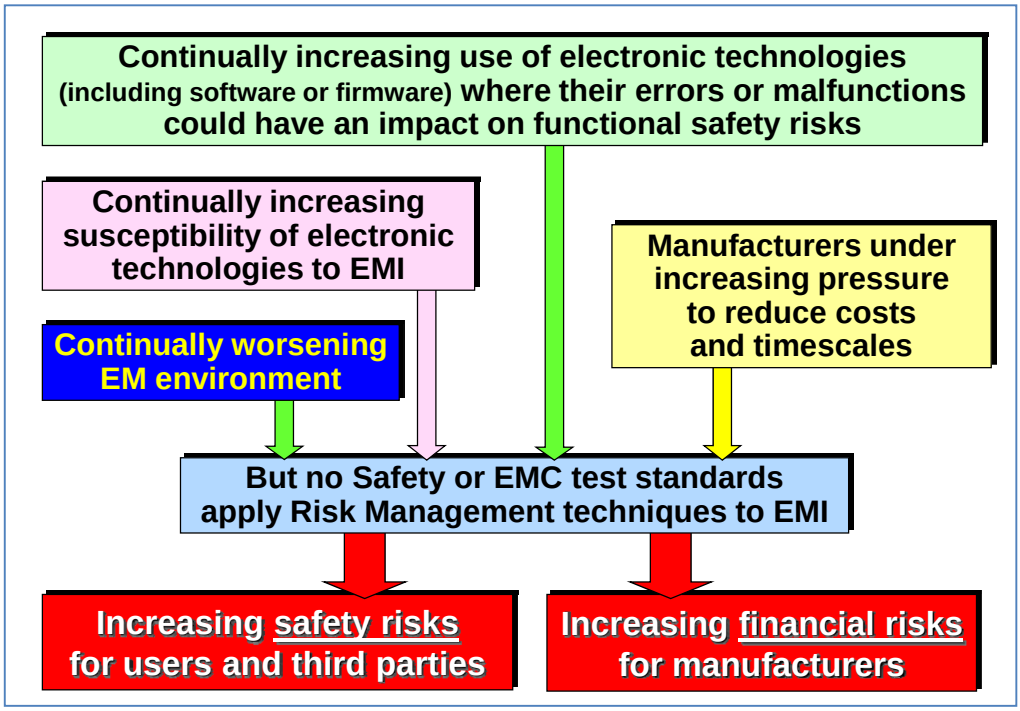

Figure 1 Increasing safety and financial risks due to EMI

This looming problem was recognised in the late 1990s, and since then the new discipline of 'EMC for Functional Safety' has been developed to help electronic systems maintain tolerable levels of safety risks.

Published in Interference Technology's 2010 Yearbook

My Working Group at the IET started work in 1998, and in 2008 produced the first ever guide on how to do EMC for Functional Safety [1].

It comprehensively describes practical and cost-effective procedures for both management and engineering, and can be used immediately to help to save lives and reduce injuries, whenever electronic technologies are used in safety-implicated products, systems or installations of any kind.

It is so practical that it even includes useful checklists to aid project management, design. and compliance assessment.

The IET Guide can also be used to improve reliability, for example in high-reliability, mission-critical, or legal metrology applications. (Although some 'fail-safe' design techniques may not be appropriate for such applications.)

When this Guide is correctly applied, real financial savings can be expected, along with a significant reduction in financial risks. (Now *there's* an interesting message to pass on to your boss!)

1 Brief Overview of the IET's 2008 Guide

Ever-more sophisticated electronic technologies (including wireless, computer and solid-state power conversion) is now commonplace, and increasing in every sphere of human activity, including those where errors or malfunctions in the technology can have implications for functional safety. Activities affected include, but are not limited to:

Commerce	Industry	Banking
Government	Security	Medicine and healthcare
Agriculture	Defense	Energy and energy efficiency
Entertainment	Leisure	

Transport: Vehicles and Infrastructure: Road, Rail, Marine, Air, Space, etc.

All electronic technologies are susceptible to suffering from errors or malfunctions caused by electromagnetic interference (EMI), and increasingly sophisticated technologies tend to be more susceptible.

As well as natural sources of EMI, such as lightning and electrostatic discharge (ESD), all electrical and electronic technologies are sources of EMI, and as electronic technologies become more sophisticated they tend to emit EMI at higher levels and/or higher frequencies. Plus, there is a huge trend towards the increasing use of wireless datacommunications and switch-mode power conversion (e.g. energy savings, "green" energy sources, electric and hybrid vehicles, etc.) – but these are inherently very noisy technologies indeed.

Functional safety engineering and EMC engineering have developed separately for decades, partly because of mandates by the International Electrotechnical Commission (IEC), but also for other reasons [2].

This means that we now have the situation that functional safety engineers do not generally have a good knowledge of EMC, and EMC engineers do not generally have a good understanding of functional safety. And, it has to be said, most "traditional" safety engineers often have a poor understanding of Functional Safety – a discipline that itself only really got going in 2000 with the publication of IEC 61508 [6].

At the time of writing (March 2010) there are no published EMC standards that are appropriate for achieving functional safety, and there are no safety standards that include appropriate EMC requirements for functional safety (mostly, they have no EMC requirements at all).

However, although it is not a published standard (yet) – we do have IEC TS 61000-1-2 [8], which was written with aim of filling a gap in IEC 61508 [6] by providing its "missing EMC Annex". The 2nd Edition of

[6], due to be published very soon (maybe during 2010) lists [8] as the document to apply to control EMC for functional safety purposes.

The IET's Guide takes [8] and develops its requirements into a 180+ page practical guide that is easy to follow, complete with checklists to aid designers, project managers and assessors. Whilst doing this, it also uses a more general terminology than [8] so that it can be used in any project, regardless of the functional safety standard being applied, whether it is IEC 61508 [6], ISO 14971 (medical) [9], ISO 26262 (Automotive) [10], IEC 60335-1 [11], IEC 61511 [36], IEC 62061 [37], or none.

The IET Guide's aim [1] is to provide management and technical tools that enable the use of electronic technologies in applications where they could have an impact on functional safety – controlling the risks due to EMI for customers and third-parties, and thereby reducing financial risks to manufacturers and service providers.

Financial risks mostly arise due to product liability legislation, but also due to safety regulations that can cause unsafe products to be banned from large markets such as the European Union (EU) and/or undergo recall. Many companies are aware that legal claims that go against them could be very costly indeed, and could also ruin their brand reputation. For this reason, they have, for decades, employed legal experts to either win cases for them, or settle out of court with binding non-disclosure agreements. In this way the true cost of poor engineering has generally been hidden from the public, government, and other companies.

At some point the costs of doing EMC engineering properly will be less than the legal costs of ignoring it (or the loss of sales due to media exposure). That point may already have been reached, because of the general financial improvements that are available from EMC engineering. [3] and [4] show that appropriate EMC engineering techniques have been available for some time, to help reduce the costs and timescales in design and development, and reduce unit manufacturing and warranty costs whilst improving functionality and maximising market share.

The Guide's methods can be used to reduce risks in high-reliability, mission-critical and legal metrology applications, as well as generally improving financial performance and market share, and will also help suppliers to the UK's military comply with Annex H of the UK's DEF STAN 59-411 Part 1 [5].

To avoid confusion with the many different terms used in electrical and electronic engineering (for example: device, apparatus, system, safety system, installation, etc.) the IET Guide coined a new acronym: 'EFS', defined as: *'Any entity employing electrical and/or electronic technologies that provides one or more functions having a direct impact on safety'.*

The intention of inventing "EFS" was to cover the entire range of constructional possibilities. Note that an EFS is *never* a component, part, element, subsystem or subset of the entity that is providing the safety function.

There are many types of organizations as well as those called "manufacturers" who could create an EFS, so to avoid confusion the Guide calls them all "EFS creators".

Figure 2 shows the nine basic steps employed by the Guide, which include checklists to aid project management, design and compliance assessment. It has been pointed out that the figure actually shows ten steps, but only nine of them are involved with actual engineering, hence the term "9-Step Process".

Figure 2 is for a 'Simple EFS', but the Guide also describes an expanded process that will handle projects of any size, with any number of levels of subcontracting, known as "Complex EFSs".

Part 2 of this article discusses how various practitioners of functional safety and/or EMC will need to learn new tricks. Part 3 shows why it is that we can no longer rely on EMC testing alone, and Part 4 provides brief descriptions of each of the steps in Figure 2.

Overview of the EMC for Functional Safety process for a 'Simple' EFS

An EFS is any entity employing electrical and/or electronic technologies
that provides one or more functions having a direct impact on safety

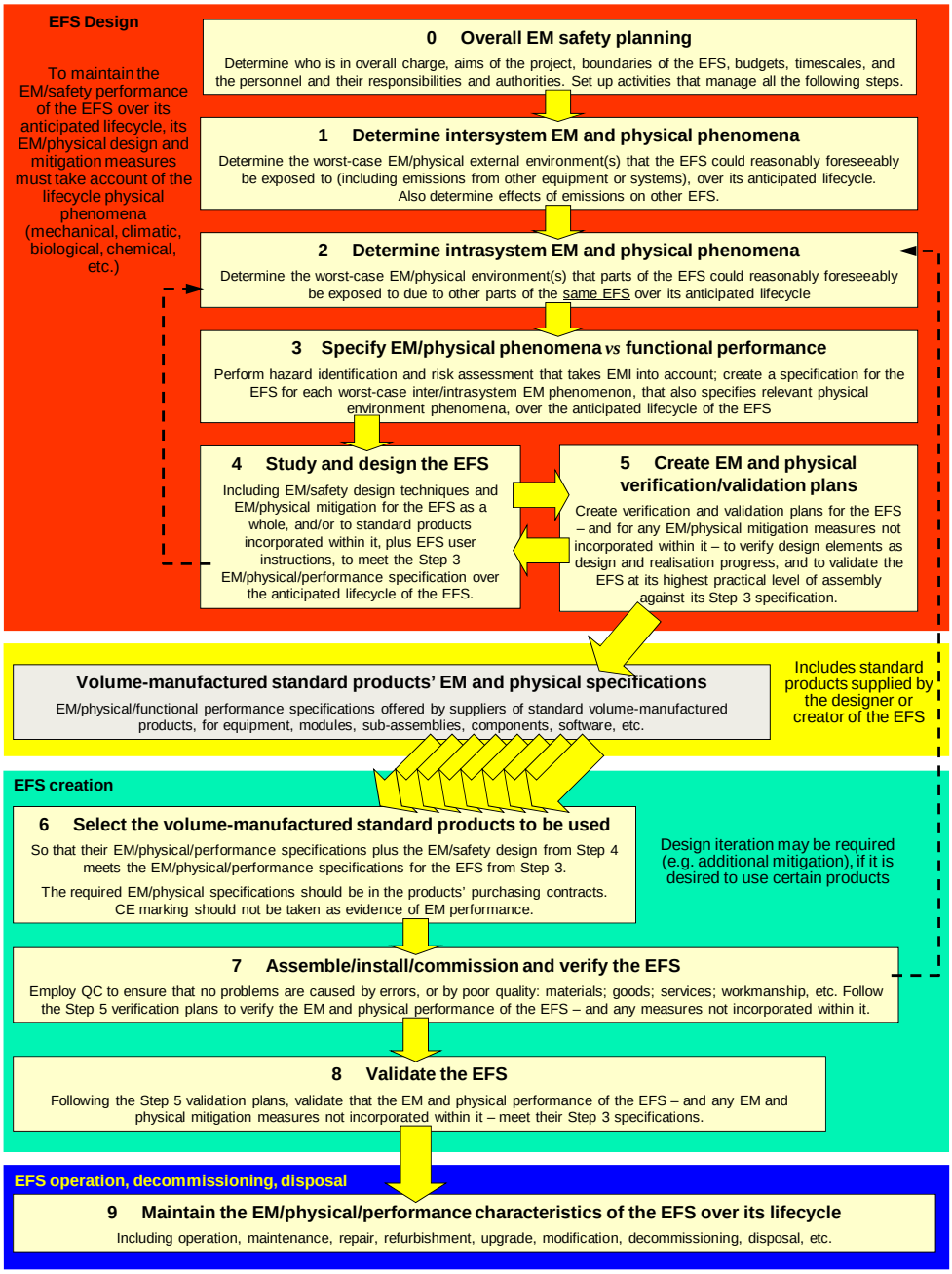

Figure 2 The IET's "9-step process" applied to a "Simple EFS"

Published in Interference Technology's 2010 Yearbook

2 Up the Learning Curve

The Guide's approach means a significant learning curve for many EFS creators. But the alternative is a future of unacceptable levels of deaths and injuries, and unacceptable financial risks and losses by both the creators and their customers or users, as shown in Figure 1.

The process described by the Guide should be clearly seen for what it really is – a methodology for improving cost-effectiveness and reducing financial risks over the medium and longer term. In fact it is much more than that – it is also a methodology for ensuring customer and investor confidence. For government bodies and other non-profit organisations it provides similar benefits.

Executives could also use it as a method for reducing their personal liability under the UK's Corporate Manslaughter Act – or similar legislation in other countries – that aims to ensure that one or more senior responsible individuals are held personally accountable when their company's actions (or inactions) cause safety accidents.

Functional safety assessors (e.g. those already qualified to assess to IEC 61508 [6] or its 'daughter' standards such as IEC 61511 [36] or IEC 62061 [37]) will need to develop the necessary skills to assess EMC for functional safety.

No doubt some EMC testing laboratories will also develop the necessary skills to assess the EMC for Functional Safety of an EFS design. Some of them will certainly want to expand their markets by offering customised EMC tests for EFS, and offer assistance in developing individual EMC for Functional Safety test plans.

3 Many reasons why EMC testing is insufficient for controlling safety risks

Also see [2] [12] [13] [14] [15] [16] and [17].

3.1 Reasonably foreseeable faults not tested

Immunity to the normal electromagnetic (EM) environment can be negatively affected by faults, for example:

- Missing or damaged conductive gaskets
- Loose/missing fixings in enclosures or cable shielding
- Failure of surge protection devices
- Intermittent electrical connections
- Dry joints, open or short circuits (e.g. in RF filters)
- Out-of-tolerance or incorrect components

Normal safety testing simulates all reasonably foreseeable faults to check if the protection that has been designed-in (usually as the result of a Failure Mode and Effects Analysis, Fault Tree Analysis, or similar) operate as intended.

But EMC immunity testing is only performed on perfect specimens of products and systems. *This is enough on its own to disqualify EMC testing as being a sufficient means, on its own, for demonstrating that EMI cannot cause excessive functional safety risks.*

In fact, the manager of an Automotive EMC Test laboratory recently told me that it is not uncommon for automotive components in serial manufacture to fail their regular quality-control EMC tests. Engineers visit the test lab, discover that the components have been assembled incorrectly – and although they function correctly, their immunity to EMC has been compromised. They correct the mistake with the component, the test is repeated and passed.

There's nothing wrong with the design – as far as passing its EMC tests is concerned, anyway – but no steps were taken in the design to provide a fail-safe or backup system for the reasonably foreseeable assembly error. Also, no steps are taken to improve the production process, so the EMC characteristics of vehicles delivered to customers are unknown.

3.2 Reasonably foreseeable use, and misuse not tested

A basic principle of good safety engineering practice (and a way to help avoid liability claims) is that tolerable safety risk levels must be maintained despite reasonably foreseeable use or misuse.

Of course, it is impossible to make anything perfectly safe – but people are known to behave in certain ways, which includes the propensity to make mistakes in certain known ways – so safety engineering takes this into account.

However, as for faults (see above), EMC immunity testing assumes that equipment is operated perfectly at all times, and will never be damaged, modified or upgraded by anyone.

3.3 Anechoic chambers not representative of real-life EM environments

Most radiated immunity test standards specify anechoic test chambers, which are unlike all real-life EM environments (except for a missile when it is flying through the air) and so their results can differ markedly from what will happen in real life.

Some manufacturers and most EMC test laboratory managers assume that increasing the test levels well beyond what will occur in real-life provides a "safety margin" (a rather unfortunate term, in this context!). Of course, testing at higher levels does improve confidence that the test level applied was actually at or above the test levels specified for the environment, as shown in Figure 3, and [18] shows that this "expanded uncertainty" is an important technique when controlling safety risks.

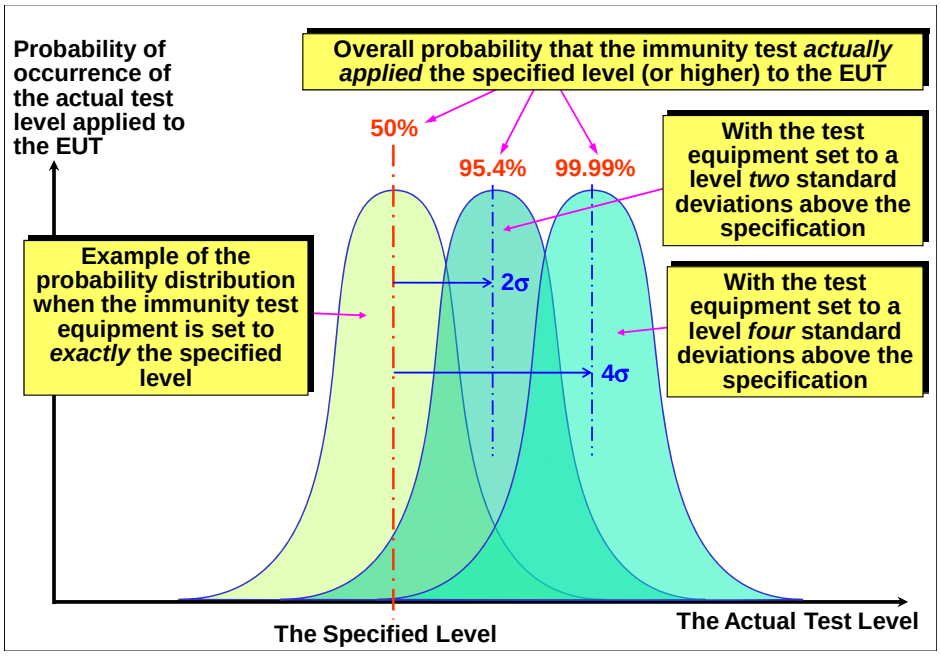

Figure 3 Using "Expanded Uncertainty" improves test confidence when testing linear systems for continuous radiated or conducted immunity

Published in Interference Technology's 2010 Yearbook

Also, if we assume that mitigation measures such as shielding and filtering will degrade by a few dB over the life of the equipment, it is reasonable to add those few dB to the test level. But what if a 60dB shield or filter suffers a catastrophic fault, or the operator leaves the shielded door open, do we test with 60dB higher levels?

For instance, instead of testing at 3V/m, add 60dB to allow for the degraded shielding or filtering, and test at 3,000V/m? And if we also want to increase the test level setting by four standard deviations to achieve 99.99% confidence that we tested at or above the specified level, do we then test at 10,000V/m?

[18] shows that testing at higher levels is no universal panacea, and describes a number of easily understood reasons as well as those discussed above.

There are also concerns about the measurement uncertainties in the test chambers, with some EMC testing experts suggesting large and unpredictable uncertainties [19] [20]. Reverberation chambers can provide much more realistic tests [21] [22], and for this reason are used by many manufacturers of flight-critical avionics and preferred by [23].

3.4 Reasonably foreseeable RF modulations not tested

For ease of testing, low costs and repeatability, standard RF immunity tests use 1kHz sinewave modulation, although some vehicle manufacturers employ pulse modulation to simulate digital cellphones and radars above about 600MHz, and military standards use 1kHz squarewave, for example [5], [38].

However, real-life environments contain EM disturbances with a range of modulation types and frequencies, as pointed out by [24]. [25] and [26] show that immunity can be significantly degraded (e.g. by 20dB or more) when EMI modulation corresponds with frequencies or waveforms used in internal processes, or resonates with circuits, cables, transducers or loads.

Modulation's importance for EM immunity has been well known in military electronic warfare for many decades, but is only now just starting to be addressed by some standards, see [23] and [27].

3.5 Reasonably foreseeable simultaneous EM disturbances not tested

EMC immunity testing applies a limited number of types of EM disturbance, one at a time. But in real-life operation, equipment is often exposed to simultaneous EM disturbances. For example: two or more RF fields at different frequencies; a radiated field plus a conducted transient or electrostatic discharge, etc. [28] shows that equipment that passes its individual immunity tests can be much more susceptible to lower levels of the same disturbances when they are applied simultaneously, as they can be in real life.

In the EMC world it is often argued that simultaneous disturbances are too unlikely, but it is pretty obvious that (for example) distorted AC mains supply waveforms occur all the time, and if this results in a lower peak level (as it often does) then the storage capacitor on the unregulated side of the DC power supply will not be charged up as much as normal, and an equipment's susceptibility to dips and dropouts in the AC supply will be different from when it is tested with a nominal supply.

It is also pretty obvious that some areas of the world suffer from quite high field strengths from nearby radio broadcast transmitters, even large parts of some cities are exposed to fields of over 3V/m at multiple broadcast frequencies at once. In such areas transients and ESD continue as normal, of course, meaning that exposure to one or more RF fields at the same time as transients and ESD is a reasonably foreseeable situation (and one that was tested by Michel Mardiguian [28] and found to cause problems).

And even independent transients will occur simultaneously on occasion. Maybe so infrequently that they can be ignored for normal purposes, but, for example, when considering a safety-related system that is made in very high volumes, like automobiles on the roads in their tens of millions, even such a very small possibility could be happening on a daily basis, and so is reasonably foreseeable and needs to be taken into account.

Published in Interference Technology's 2010 Yearbook

Simultaneous disturbances with different frequencies can cause EMI through intermodulation (IM), which (like demodulation) occurs naturally in non-linear devices such as semiconductors. Figure 4 shows a simple example of two RF fields at different frequencies, which can cause EMI by:

- Direct interference from each frequency independently
- Demodulation of the amplitude envelopes of either frequency, or both mixed together
- Intermodulation, in which new frequencies are created

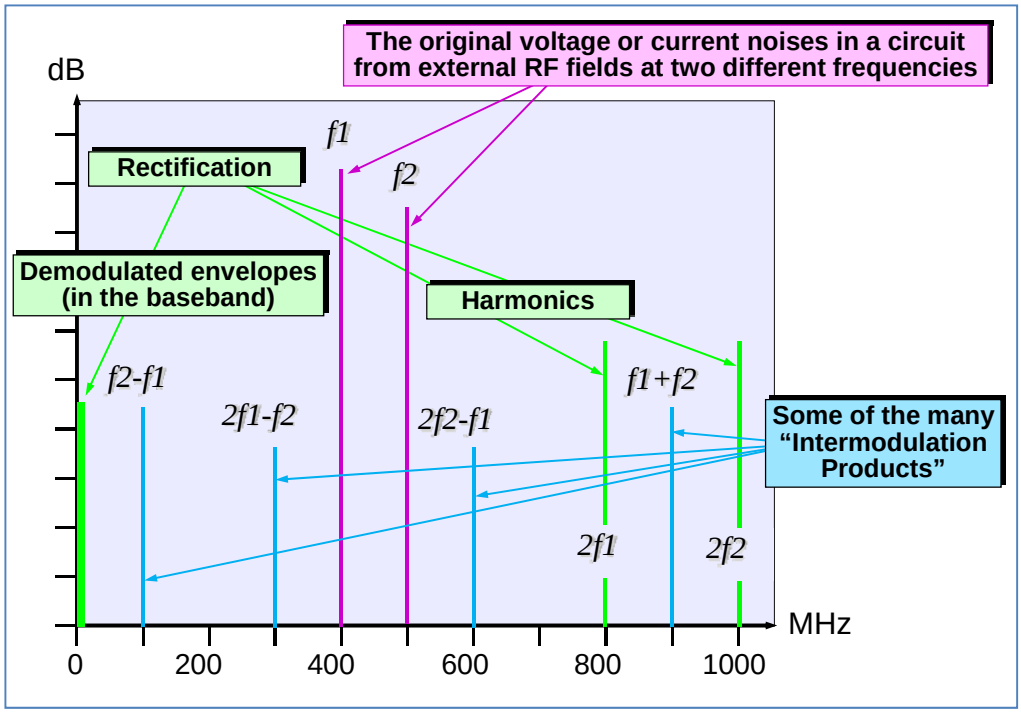

Figure 4 Example of demodulation and intermodulation

Imagine we perform normal radiated immunity testing over the frequency range 150kHz – 6GHz, and discover that our product is too susceptible over 10 – 200MHz. Being competent EMC engineers we add or modify shielding and filtering to make it effective over the susceptible frequency range, so that the equipment now passes the test. We pat ourselves on the back, and proceed to the next test, or the next product.

We didn't bother to improve the mitigation over the range 200MHz – 6GHz, because it was not needed to pass the test. Why waste the time, and add unnecessary cost? But in real life, simultaneous noises in the frequency range 200MHz – 6GHz *will* occur, and *will* enter the product, where they *will* intermodulate, with some reasonably foreseeable probability of creating *internal* noises in the 10 – 200MHz range and causing the very interference we were so pleased that we had stopped. [18] shows that that the original test might never discover this problem, no matter how high its test level.

3.6 Only one port tested at a time

An item of equipment subjected to a radiated EM field picks up RF voltages on all of its cables, with phase differences between them due to their different routing, stray capacitances, etc. But conducted immunity tests only apply RF stresses to one cable at a time.

Published in Interference Technology's 2010 Yearbook

Qinetiq PLC (in the UK) tell me that they have injected RF energies into all of an equipment's conductors simultaneously, but with phase shifts to match what would be expected in real life. They discovered that the immunity could be significantly worse than when one cable was tested at a time when following the standard immunity test methods. (Unpublished work at the time of writing.)

3.7 Reasonably foreseeable physical/climatic effects not tested

For safety, it is important to maintain an appropriate level of EM performance over the anticipated lifecycle, despite the reasonably foreseeable effects of physical and climatic environments, including the following:

- Mechanical
  (e.g. static forces (bending, twisting) , shock, vibration, etc.)
- Climatic
  (e.g. temperature, humidity, air pressure, etc. – both extremes and cycling effects)
- Chemical (e.g. oxidation, galvanic corrosion, conductive dusts, condensation, drips, spray, immersion, icing, etc.)
- Biological
  (e.g. mould growth, rodent gnawing, etc.)
- Operational "wear and tear" over the lifetime
  (e.g. friction, fretting, repetitive cleaning, grease build-up, etc.)
- Ageing and corrosion

Foreseeable effects vary from immediate (e.g. non-flat mounting opening a gap and degrading shielding), to long-term (e.g. corrosion of a shield joint or filter ground bond). MIL-STD-464 [29] describes a number of real-life problems of this nature; [30] and [31] are also relevant, as is the last paragraph of [32].

[33] shows that up to 20dB degradation in filter attenuation can be caused by combinations of ambient temperature, supply voltage and load current within the filter's ratings – compared with the results of the normal immunity tests.

Highly-accelerated life testing (known as "HALT") is already performed by some manufacturers, to check that functionality is maintained over the anticipated lifecycle, but the resulting "pre-aged" units are not then tested to see if their EM characteristics have degraded by too much, even in the avionics and military industries. However, I am told that the Russian Military take their equipment after simulation of their lifetime physical and climatic exposure, and run their EMC tests again to check they still meet the specs.

3.8 Quality of EM engineering design ignored by EMC testing

It is very common for manufacturers to EMC test their products, iterating their designs until they pass. Apart from being a very bad use of resources and running huge financial risks [4] – this might not reveal whether the pass was achieved by good EM design, or by something that would not be adequately controlled in serial manufacture over the production life.

For example, if a product's EM design does not cope with component tolerances, semiconductor die-shrinks, variations in assembly (e.g. cable harnesses, grounding, etc.), replacement of obsolete components, firmware bug fixes, etc., then reasonably foreseeable variations in serial manufacture could degrade its EM characteristics and worsen safety risks.

Just because one or two samples of a product passed their EMC tests means *nothing at all* for the EM characteristics of the products actually supplied, unless its design has taken care of the above variability issues.

This is, of course, a general issue for any system integrator – even if you go to the trouble of checking that the correct EMC tests *really were* carried out and *really were* passed, for the units you are planning to buy to assemble your system – how can you be sure that the units supplied would pass the same tests? Remember the automotive EMC test lab manager's story at the end of 3.1.

And (under EU Directives, if not in other countries), it is the company that placed the finished equipment on the market who is liable for all of its safety and EMC. In the case of non-compliance, they can't simply point official investigators back down the supply chain and expect to avoid prosecution themselves. All system integrators are assumed to be professionals, and as a result be fully aware of issues such as those just discussed.

3.9 Reasonably foreseeable assembly errors not tested for

Good safety engineering always requires some basic testing of each unit manufactured to make sure that assembly errors have not made it unsafe. But standard EMC tests do not include any requirements for manufacturers to perform routine checks on EM characteristics in serial manufacture.

Test laboratories say that it is not uncommon for items of equipment that function correctly to fail EMC tests because of "misbuild". Although most manufacturers employ rigorous end-of-line testing, including in-circuit tests that will discover misbuilds that affect functionality, they almost never aim to discover misbuilds that can affect EMC characteristics, which can then affect safety risks.

3.10 Systematic effects not tested

The general assumption is that if all of the products incorporated into a system pass their immunity tests individually, then the systems thus created will also be immune enough and would pass their immunity tests. The assumption is that there is then no point in testing the completed systems, because they would be bound to pass.

But these assumptions are completely wrong.

Performance degradations that are perfectly acceptable when an item of equipment is EMC tested, or are not even measured during the testing, could have significant implications for the functional safety of systems that use them.

A good example is a 3.3V DC power supply unit used to power a microprocessor-based unit. When tested to IEC 61000-4-4 (fast transient burst) the power supply output hiccups – goes to zero for a few hundred milliseconds and then automatically recovers. The manufacturer agrees that this meets Performance Criterion B, which is all that is required. When the microprocessor unit is tested to IEC 61000-4-4, nothing goes wrong with it at all.

But put the two units together to control a robot and apply the same test to this simplest of systems, and the micro will crash and take tens of seconds to reboot, whilst the system it is controlling goes haywire and perhaps lays waste to all around it, including any poor individuals within reach of its arms.

It is in fact a common experience that, when systems are tested, there is very poor agreement between the EMC test results on items of equipment, and on the systems that are constructed with them [34].

3.11 Maximum test level not necessarily worst-case

Electronic devices are all non-linear, and circuits/firmware can be very complex, so products can sometimes fail when tested with low-level EM disturbances – but fail in a different way – or even pass when tested with the maximum specified levels.

But many EM immunity tests only expose equipment at the highest specified level, to save testing time and cost.

Lower disturbance levels will usually be much more likely in real life, and so could be much more significant for functional safety.

3.12 Conclusion – EMC immunity testing is never sufficient on its own for safety

I hope I have shown that EMC testing can *never be sufficient* – on its own – to demonstrate that functional safety risks are low-enough, or that risk-reduction will be high enough, over the lifecycle of an EFS, taking its physical and climatic environments (including wear and ageing) into account.

The number of variables is simply too large. Test plans could be drawn up which would provide the necessary design confidence, but no-one (even governments) could afford their cost, or the very long time they would take.

But we've been here before! In the 1990s it was realised that testing was not sufficient to demonstrate that software programs were reliable enough for use in safety systems. After many hundreds of man-years of work by academia and industry, the result was Part 3 of IEC 61508 [6].

What is required to do EMC for Functional Safety is to adopt the approach that has been taken in every other aspect of safety engineering (including software, since 2000) of employing proven good engineering techniques such as risk management, using a wide range of verification and validation methods.

Verification and validation will still involve some EMC testing – maybe quite a lot of it – but the point is that it will probably be carefully tailored for each project, to provide confidence in the safety design and manufacture where the other verification and validation techniques are not able to give us the confidence we need for the level of risk (or risk-reduction) that is our target.

They will generally not be just a fixed set of EMC tests. (This should be good news for test lab managers and engineers everywhere – something to engage their brains instead of simply repeating the same boring tests day after day after day!)

To put it a different way, doing EMC for Functional Safety means that we need to apply Risk Management methods – such as those in IEC 61508 [6] – to EMC. This was exactly the approach that was taken by IEC 61000-1-2 [8], and also by the IET's Guide that is the subject of this paper [1].

4 Discussing the Steps in the IET's Guide

4.1 Step 0: Managing the 9-step Process

The IET's new Guide requires that an organisation with responsibility for any of the activities within the scope of the Guide's process, should appoint one or more persons to take overall responsibility for:

- The EFS, or for all relevant activities
- Coordinating the EMC-related activities
- The interfaces between those activities and other activities carried out by other organisations
- Carrying out all the requirements of this Step
- Ensuring that EMC is sufficient and demonstrated in accordance with the objectives and requirements of the IET's Guide

Responsibility for EMC-specific functional safety activities may be delegated to other persons, particularly those with relevant expertise, and different persons could be responsible for different activities and requirements. However, the responsibility for coordination, and for overall EMC for functional safety, should reside in one or a small number of persons with sufficient management authority.

As with all safety engineering undertakings, the time, effort, and skill required for performing and managing an activity depends upon the level of safety risk (or risk-reductions) considered acceptable for

the EFS. Lower levels of risks require greater confidence in design and verification – hence more work and more thorough documentation.

4.2 Step 1: Determine the Intersystem EM and Physical Phenomena

The IET's Guide accepts that an EFS may need to maintain certain minimum levels of EM immunity despite *at least one* fault, such as the wear-out of a surge protection device by the surges it is exposed to over time. Another example is a broken filter ground connection, which could be caused by poor assembly; shock, vibration, or corrosion over the lifecycle; or wilful damage.

EFS designers need to know enough about their equipment's "environment" (EM; physical; climatic; wear; ageing, etc. over the anticipated lifecycle) and foreseeable faults and misuse, to select appropriately-rated components, and to design circuits, software, filtering, shielding, overvoltage protection, etc. They need this information to be able to achieve the reliability required for operational functions that could have an impact on safety over the entire lifecycle.

For example, engineers need enough information to be able to design:

- EFS and its EM/physical mitigation techniques to cope with the foreseeable range of EM disturbances over the anticipated lifecycle of the EFS, including low-probability events (how low depends on the safety requirements of the EFS) and simultaneous EM disturbances.
- Feedback circuits – so that they do not become unstable due to temperature variations affecting component parameters (e.g. gain-bandwidth product, phase margin, etc.).
- Filters – so that vibration and corrosion will not cause their ground bonds to degrade; and that variations in supply voltage, load current and temperature do not degrade their attenuation too much [33].
- Shield joints and gaskets – so they will continue to perform as required despite twisting of the frame due to mounting on non-flat surfaces; and will withstand wear and tear, corrosion, mould growth or other lifecycle influences [30].
- Surge protection that will withstand the foreseeable overvoltages and overcurrents for the lifecycle of the EFS, or at least for the period between maintenance activities.
- EFS and its EM/physical mitigation techniques so that their EM and physical characteristics will not be unacceptably degraded by lifecycle activities such as: maintenance; repair; refurbishment; modification; upgrade; decommissioning, etc.
- etc.

They also need this information to create a test plan for both EMC and HALT that will verify/validate the design, and to design the routine EMC testing and physical stress screening required in volume manufacture.

The EM/physical environments that exist without the EFS in place are called *intersystem* environments, and are the subject of Step 1 in this EMC for functional safety process. Where the statistical distribution of an EM, physical or climatic "threat" is not known, the reasonably foreseeable worst-case value that could possibly occur during the lifecycle should be determined with sufficient accuracy, and the design based on that. Figure 5 shows some of the EM issues that should be taken into account when assessing an intrasystem EM environment.

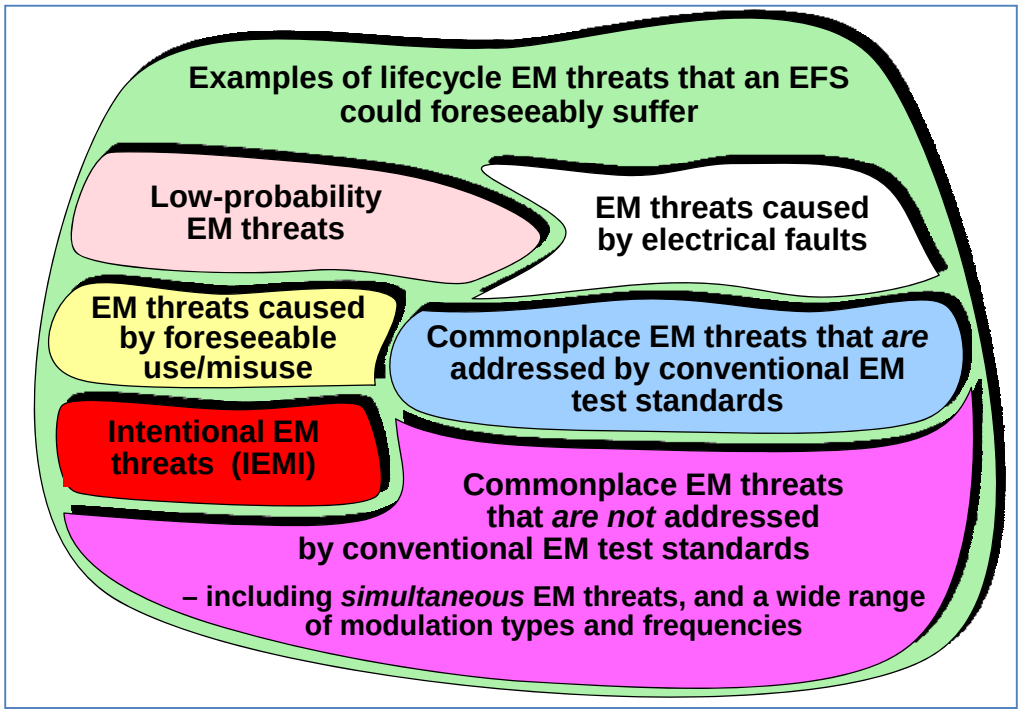

Figure 5 Some of the EM environment issues to be taken into account

4.3 Step 2: Determine the Intrasystem EM and Physical Phenomena

Each item of electrical/electronic equipment creates its own EM and physical disturbances, and so has an effect on its local EM/physical environments. Where an EFS is comprised of several items of equipment, the emissions from one or more of them might interfere with one or more of the other parts of itself. This is known as *intrasystem* interference, and is the subject of this step.

Where the statistical distribution of an EM, physical or climatic threat is not known, the worst-case value that could possibly occur during the lifecycle should be determined with sufficient accuracy, and the design based on that. The combination of the worst-case intersystem and worst-case intrasystem environments should be captured in the environmental specifications that are the output of Steps 1 and 2 to the rest of the EMC for functional safety process.

4.4 Step 3: Specify EM/Physical Phenomena vs Functional Performance

No EMC or safety standard can ever specify exactly what is required for a given EFS, because to be adopted internationally it must inevitably adopt a general approach and strike a balance between under-engineering and over-engineering, often called a technical/economic compromise. Competent engineers should therefore carefully assess each EFS with respect to its operational situations. This Step in the EMC for functional safety process creates an “EMC safety specification” that helps a given EFS achieve tolerable levels of safety risks, or risk-reductions. It is also part of a process that helps ensure the amount of safety engineering is just right, so that under- and over-engineering is avoided.

Steps 1 and 2 assessed the worst-case EM and physical environments over the anticipated lifecycle. The outputs from these Steps are specifications for the worst-case EM and physical environments. Where

appropriate, it can help to base these specifications on existing standards (such as the DEF STAN 59-411 [5], MIL-STD-461F, the IEC 61000-4 series or IEC 60721 series [35]), competently modified as necessary. Doing this can make it easier to verify and validate the design by testing, in Steps 7 and 8, because test laboratories and equipment hire companies (and many manufacturers) will already have much of the equipment and expertise necessary to apply those test methods.

This Step 3 is concerned with creating the EMC safety specification for the EFS, which will include both EM and physical specifications, and upon which Steps 4 and later steps all depend.

Where an EFS creator subcontracts part of the design, the subcontracted item requires an Item Requirement Specification (IRS) that helps to ensure that the overall EFS complies with its EMC safety specifications, see Step 6 in Section 5.7.

4.5 Step 4: Study and Design the EFS

It is important to ensure that EFS do not become unsafe as a result of EMI due to their EM environment (including EMI they create themselves). It is also important to ensure that the EM emissions from a new EFS (or part of it) do not increase safety risks by interfering with existing EFSs. Accordingly, it is the responsibility of the EFS designer (which may be a team of people) to apply appropriate EM/physical measures throughout the lifecycle of the EFS.

Where it is not within the authority of the designer to apply a certain measure (e.g. repair of an EFS after it has been sold to another company), the designer should provide appropriate and clear instructions on what should be done, and by whom, with clear warnings about the potential consequences for safety risks (or risk-reductions) of failing to follow them.

In most cases, mass-produced electrical, electronic or programmable electronic products and other devices and interconnections that are often used to assemble an EFS cannot be expected to have EM emissions and/or immunity characteristics that are adequate for all of the possible EM environments that an EFS might experience. Therefore, it is important to recognize that EM and/or physical mitigation measures, applied at the level of the equipment, system and/or installation, are often an effective way to achieve the required characteristics for the target level of safety risk.

One aim of this Step in the Guide is to provide an overview of some of the measures and techniques that are available for the achievement of functional safety with regard to EMI. It cannot specify how to design an EFS, because each EFS and its application and EM/physical environment is so different. Instead, it discusses the major design issues and some techniques by which they may be addressed.

Whilst the IET Guide describes many design techniques that can be used in Step 4, it is not comprehensive; there are other techniques that could be equally effective. They are just a list of some techniques that have been found useful in the past, and there is no obligation to use all or any of them. Some of these techniques might not be suitable for some types of EFS. How the EFS designer ensures that the desired levels of safety risks (or risk-reductions) are achieved over the anticipated lifecycle is entirely up to him or her.

Performing a risk assessment for EMC for functional safety generally requires using *at least one* “bottom-up” (inductive) method, such as FMEA, Event Tree Analysis, etc., plus *at least one* “top-down” (deductive) method, such as Fault Tree Analysis. Also required is “brainstorming”, using a wide variety of participants (not just designers), plus Task Analysis, Human Reliability Analysis, and other methods where relevant. But the normal, standardized risk assessment methods were never designed to cover EMI issues, so need competently adapting to take into account, for example:

- “Latch-up” (all integrated circuit pins pulled low simultaneously by a malfunction inside itself)
- “Common-mode” disturbances (which affect two or more subassembly ports or circuit nodes simultaneously)

- EMI and intermittent contacts, which can create noises that can be mistaken for valid signals
- Multiple simultaneous faults (unless their probability is shown to be low enough, over the anticipated lifecycle, to treat them one-at-a-time)
- Etc.

When presenting papers and discussing EMC for Functional Safety, as I have been for 10 years now, I sometimes meet people dismiss me as some crank who wants to make everything perfectly safe. Well, we all know that nothing can ever be perfectly safe, and the IET's Guide is no exception.

The whole point of [6], [8] and the 2008 Guide is to spend money and time wisely, to make things that are no more costly then they need to be to achieve an appropriate level of safety risk. To take some medical examples, one day we might be using the IET's Guide to help design a product that will be used on babies and young children, where the "tolerable risks" we are prepared to accept are very low indeed.

But another day we might be using the Guide to help design a medical device that will be used to try to extend the lives of people who otherwise have only a couple of days to live. For such devices, a very high probability of dying as a direct result of a malfunction in the device might be acceptable – maybe as much as 50% in some situations.

4.6 Step 5: Create EM and Physical Verification/Validation Plans

As was shown in Section 4 of this paper, EMC testing can never be sufficient on its own to demonstrate that risks are low enough, or that risk-reduction will be high enough, over the lifecycle of an EFS, taking its physical environment (including wear and ageing) into account. Test plans could be drawn up which would provide the necessary design confidence, but no-one (even governments) could afford their cost, or the very long time they would take.

No other safety engineering discipline, including software, ever relies totally upon testing a finished product. In fact it is very well recognised in safety engineering, and especially in functional safety engineering, that testing alone is insufficient. What they employ instead, and we now need to apply to EMC, is competent design engineering, plus a variety of verification and validation techniques, which will include some carefully-targeted testing.

Different designs of EFS may employ modified or different design techniques (see Step 4 of the Guide) and/or be used in different applications – but to be time- and cost-effective we must accept that no single design methodology will be found to be suitable for *all* types of EFS.

Where EFS designs and/or applications differ, verification and validation techniques may need to be adapted – and different techniques may need to be employed. The EMC testing employed may need to be adapted, or different tests applied. No one verification/validation plan or EMC test methodology is suitable for all designs of EFS (to be time- and cost-effective).

Step 4 of the Guide's 9-step process (see Figure 2) designed the EFS, using techniques as appropriate to its application, functions, and the EM/physical requirements of its EMC safety specification and risk assessment (from Step 3).

Step 5 now deals with planning the verification and validation of the EFS design, including its EMC testing, against the EM/physical requirements of its EMC safety specification (from Step 3). Most of the text and graphics in this Step deal with EMC testing issues, but that does not mean that testing is the most important verification and validation method of the several that must be applied. For example: Expert Review is often found to be the most powerful method for detecting design errors, and also one of the quickest and most cost-effective.

The planning of the validation and verification techniques needs to be performed by competent and knowledgeable personnel during the design phase (Step 4), because the two steps are interactive. It can be possible to avoid lengthy and expensive verification and validation programmes by doing the design in

a different way, and employing certain verification and validation techniques can sometimes allow design to proceed faster, or lower-cost parts to be used.

4.7 Step 6: Selecting Standard Products / specifying Custom Hardware or Software

Step 6 applies only where the EFS designer(s) permits the EFS creator to have such freedom of choice. In some EFS designs, especially simpler ones, some EFS designer(s) will completely specify everything about the EFS, including any standard volume-manufactured or custom-engineered items of hardware or software that are to be incorporated within it. The EFS creator then has no flexibility in this regard and Step 6 does not apply to that EFS.

This Step of the process is concerned with selecting standard volume-manufactured items of hardware or software and/or specifying custom-engineered items of hardware or software, for incorporation into the EFS by the EFS creator (who may or may not be the same company as the EFS designer(s)).

The aim of this step is to ensure that – taking into account the EM/safety design of the EFS – the EM/physical/climatic performance of any standard volume-manufactured or custom-engineered items of hardware or software incorporated into the EFS do not prevent it from meeting the EM safety specification of the EFS (from Step 3).

The required EM/physical performance specifications should be in the purchasing contracts for the standard products or custom items, and “CE marking” or Certificates of Compliance should never be taken as evidence of EM performance.

Remember: an EFS is *never* a component, part, subset, or a purchased standard product or custom-designed item that is incorporated into something else – it can *only* be the finished, complete entity that, when finally installed, is what provides the function that has a direct impact on safety risks, or risk-reductions.

4.8 Step 7: Assemble, install, commission and verify the EFS

A very wide variety of assembly, installation, commissioning and verification activities are possible in this Step. Some of them might take place on the manufacturer’s site (or manufacturers’ sites), and some on the operational site (including fixed locations, vehicles, vessels, etc.), depending on the type of EFS and the way it is designed.

These activities all fall within the lifecycle phase known as “Realization” in [6], and include such concepts as manufacture and integration. They are all specified by the design and verification documents created during Steps 4 and 5, in order to meet the specifications created by Step 3, so that the EFS achieves the desired levels of safety risk, or risk-reduction, over its lifecycle.

4.9 Step 8: Validating the EFS

This is the Step in which the finished, fully functioning EFS is validated as complying with its Step 3 requirements for safety risks and/or risk-reductions over its lifecycle, by implementing the validation plans from Step 5.

Where the EFS is large, or is a distributed system, EMC testing of its final build stage might be impractical and/or there may be no standard test methods that are suitable. A wide variety of validation activities are available for use in this Step (see Step 5) depending on the type of EFS and the way it is designed, to support whatever testing is practical (and affordable) to achieve sufficient confidence in the safety risks, or risk-reductions, achieved by the EFS.

Published in Interference Technology’s 2010 Yearbook

4.10 Step 9: Maintain EM and Physical Performance Characteristics over the Lifecycle

An EFS must maintain certain levels of safety risks and/or risk-reductions over its entire lifecycle, which of course, includes operation, maintenance, repair, refurbishment, and modifications and upgrades to its mechanics, electrical and electronic hardware and software. It must also remain safe enough during dismantling and disposal. The safety of everyone who could be exposed to risks from the EFS in any of its lifecycle phases must be controlled, by appropriate design and/or management procedures.

For example: where an EFS is controlling a powerful robot, during certain lifecycle activities (other than operation) it may be acceptable to remove the power to its motors and actuators, so that if the EFS suffers interference (e.g. due to the door of a shielded enclosure being opened) the robot cannot make any unintended or erroneous movements. If the robot needs to be operated whilst a shielded enclosure door is open, it may be acceptable for the person in charge of that activity to clear the area of any radio transmitters, or clear the area reachable by the robot of any personnel, both of them being precautions that are not taken during normal operation.

Different types of personnel perform the various activities during these phases of the lifecycle. For example: an operator will have a different set of skills, competencies and experiences than someone performing a repair or installing an upgrade, and will generally (but not always) be exposed to safety hazards for a shorter time. For this, and other reasons, the levels of safety risk or risk-reduction that are necessary for the EFS during various post-manufacture activities could be different from those that are necessary during operation.

Dismantling and disposal lifecycle phases often require no safety precautions, but the issue should always be addressed because sometimes they can. For example: nuclear power plants can take a long time to dismantle and dispose of, and certain types of EFS (e.g. cooling systems, safety interlocks, radiation alarms, etc.) need to remain operational and provide the required level of safety risks (or risk-reductions) during part or all of those phases.

5 Helpful Annexes and Checklists

The IET's new guide provides everything necessary to use it in real-life projects, and to assist those who might be unfamiliar with the topics of EMI and EMC.

It includes a comprehensive glossary of terms and acronyms, a basic understanding of what EMI phenomena can occur and how they can affect equipment, and comprehensive checklists, one for each Step in the Guide's "9-step process", which may be used by designers, project managers, and as an aid to assessors in certain types of verification and validation activities.

6 References

[1] The IET's "Guide on EMC for Functional Safety", August 2008, ISBN 978-0-9555118-2-0, available as colour-printed book from http://www.emcacademy.org/books.asp, or as free download from www.theiet.org/factfiles/emc/index.cfm.

[2] D A Townsend *et al*, "Breaking All the Rules: Challenging the Engineering and Regulatory Precepts of Electromagnetic Compatibility", 1995 IEEE International EMC Symposium, Atlanta, pp 194 – 199

[3] Keith Armstrong, "Profit from EMC", IEE Review, July 1994, EMC Supplement: pp S-24 and S-25, www.theiet.org

[4] Keith Armstrong, "When the going gets tough – smarter design wins", The EMC Journal, Edition 81, March 2009, pages 21-24, www.theemcjournal.com

[5] Ministry of Defence, Defence Standard 59-411, "Electromagnetic Compatibility", generally known as DEF STAN 59-411, available from www.dstan.mod.uk

[6] IEC 61508, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems”, in seven parts, www.iec.ch

[7] The EMC Directive 2004/108/EC and its official guide:
http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_390/l_39020041231en00240037.pdf
http://ec.europa.eu/enterprise/electr_equipment/emc/directiv/dir2004_108.htm#guide

[8] IEC TS 61000-1-2, Ed.2.0, December 2008, “Electromagnetic Compatibility (EMC) – Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena”, www.iec.ch

[9] ISO 14971, “Medical Devices – Application of risk management to medical devices”, www.iso.org

[10] ISO 26262 (draft), “Road vehicles - Functional safety”, www.iso.org

[11] IEC 60335-1, “Household and similar electrical appliances. Safety. General requirements”, www.iec.ch

[12] Keith Armstrong, “Why EMC Immunity Testing is Inadequate for Functional Safety”, 2004 IEEE Int’l EMC Symp., Santa Clara, Aug. 9-13 2004, ISBN 0-7803-8443-1, pp 145-149. Also: Conformity, March 2005, http://www.conformity.com/artman/publish/printer_227.shtml

[13] Keith Armstrong, “Functional Safety Requires Much More Than EMC Testing”, EMC-Europe 2004 (6th International Symposium on EMC), Eindhoven, The Netherlands, Sept. 6-10 2004, ISBN: 90-6144-990-1, pp 348-353.

[14] Keith Armstrong: “EMC in Safety Cases — Why EMC Testing is Never Enough”, EMC-UK 2007 Conference, Newbury, UK, Defence & Avionics session, October 17, 2007.

[15] Keith Armstrong, “EMC for Functional Safety”, Keith Armstrong (a half-day paper) 2004 IEEE Symposium on Product Safety Engineering, Santa Clara, August 13-15 2004

[16] David Pommerenke *et al*, “Characterization of Human Metal ESD Reference Discharge Event and Correlation of Generator Parameters to Failure Levels — Part I: Reference Event”, and “Part II: Correlation of Generator Parameters to Failure Levels”, IEEE Transactions on EMC Vol. 46 No. 4 November 2004, pp 498-511

[17] Simon J Brown and Bill Radasky, “Functional Safety and EMC”, IEC Advisory Committee on Safety (ACOS) Workshop VII, Frankfurt am Main, Germany March 9/10 2004

[18] Keith Armstrong, “Why Increasing Immunity Test Levels is Not Sufficient for High-Reliability and Critical Equipment”, 2009 IEEE Int’l EMC Symp., Austin TX, Aug 17-21, ISBN: 978-1-4244-4285-0

[19] L Jansson and M Bäckström, “Directivity of Equipment and its Effect on Testing in Mode-Stirred and Anechoic Chamber”, IEEE Int’l EMC Symposium, Seattle, WA, Aug. 1999.

[20] G J Freyer, “Distribution of Responses for Limited Aspect Angle EME Tests of Equipment with Structured Directional Directivity”, The 2003 Reverberation Chamber, Anechoic Chamber and OATS Users Meeting, Austin, TX, April 2003.

[21] G J Freyer and M.O. Hatfield, “An Introduction to Reverberation Chambers for Radiated Emission/Immunity Testing”, ITEM 1998,
www.interferencetechnology.com/ArchivedArtcles/shielded_rooms_and_enclosures/I98art15.htm?regid=

[22] G J Freyer, “Considerations for EMC Testing of Systems with Safety and/or Reliability Requirements”, EMC Europe 2004, Eindhoven, The Netherlands, Sept. 6-10 2004.

[23] RTCA/DO-160F December 6, 2007, “Environmental Conditions and Test Procedures for Airborne Equipment, Section 20, Radio Frequency Susceptibility (Radiated and Conducted)”. Clauses 20.4 and 20.5 attempt to cover the sensitivity of equipment to modulation type or frequency.

[24] Ron Brewer, “EMC Failures Happen”, Evaluation Engineering, December 2007, http://www.evaluationengineering.com/features/2007_december/1207_emc_test.aspx

[25] S Wendsche and E Habiger, “Using reinforcement learning methods for effective EMC immunity testing of computerised equipment”, Proc. Int. Symp. EMC (ROMA’96), Rome, Italy, Sept 1996, pp.221-226.

[26] R Vick and E Habiger, “The dependence of the immunity of digital equipment on the hardware and software structure”, Proc. Int. Symp. EMC, Beijing, May 1997, pp 383-386.

[27] DaimlerChrysler Joint Engineering Standard DC-10614, “EM Performance Requirements --- Components, 2004-01”. Clause 7 attempts to address modulation type and frequency.

[28] Michel Mardiguian, “Combined Effects of Several, Simultaneous, EMI Couplings”, 2000 IEEE Int’l EMC Symp., Washington D.C., Aug 21-25, ISBN 0-7803-5680-2, pp. 181-184.

[29] MIL-STD-464, “Electromagnetic Environmental Effects – Requirements for Systems”, Department of Defense Interface Standard, March 18 1997.

[30] L Sjögren, M Bäckström, “Ageing of Shielding Joints, Shielding Performance and Corrosion”, IEEE EMC Society Newsletter, Summer 2005, www.ieee.org/organizations/pubs/newsletters/emcs/summer05/practical.pdf

[31] W.H. Parker, W. Tustin, T. Masone, “The Case for Combining EMC and Environmental Testing”, ITEM 2002, pp 54-60, http://subscribe.interferencetechnology.com/ArchivedArticles/test_instrumentation/i_02_10.pdf?regid=

[32] J Rajamäki, “Correlations Between EMI Statistics and EMC Market Surveillance in Finland”, 2004 IEEE International EMC Symposium, Santa Clara, August 9-13 2004, ISBN 0-7803-8443-1, pp 649-654

[33] F Beck and J Sroka, “EMC Performance of Drive Application Under Real Load Condition”, Schaffner Application Note 11 March 1999; EMC Zurich, 2001; Power Quality, June 2001.

[34] T Schrader *et al*, “On-Site EMC Testing and Interference Prevention”, 2009 IEEE Int’l EMC Symp., Austin TX, Aug 17-21, ISBN: 978-1-4244-4285-0

[35] IEC 60721, “Classification of environmental conditions”, www.iec.ch

[36] IEC 61511, “Functional safety - Safety instrumented systems for the process industry sector”, www.iec.ch

[37] IEC 62061, “Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems”, www.iec.ch

[38] MIL STD 461F, 10 December 2007, “Department of Defense Interface Standard – Requirements For The Control Of Electromagnetic Interference Characteristics of Subsystems and Equipment”