emc STANDARDS

Another EMC resource
from EMC Standards

The first practical techniques for achieving EMC for Functional Safety - EMC Journal 2013

Helping you solve your EMC problems

1 Brassey Road, Old Potts Way, Shrewsbury, SY3 7FA T:+44 (0) 1785 660 247 E:info@emcstandards.co.uk

The first practical techniques for achieving EMC for Functional Safety (without using ‘big grey boxes’)

Keith Armstrong, www.cherryclough.com

First published in The EMC Journal, Issue 108, September 2013
(Reference [19] updated 18 January 2016)

Contents

Page No.

1 A quick overview

I’ve been working on ‘Electromagnetic Compatibility (EMC) for Functional Safety’ since 1997, when I persuaded the IEE (as the IET was called then) to set up a Working Group on this increasingly important issue. The IEE/IET WG on EMC4FS (as we abbreviated it) has now published three professional guidance documents:

- the first in 2000 [1], which I now find very embarrassing indeed;
- the second in 2008 [2] [3] [4], which is excellent but – as it turns out – unworkable in practice, and so is also rather embarrassing;
- the third in 2013 [5], which at long last details a practical and cost-effective approach (other than using ‘big grey boxes’ such as the military have been using for decades).

The third guidance document is called “Overview of techniques and measures related to EMC and Functional Safety”, and was created under the chairmanship of Dave Imeson, instead of me, which may be why it is so good!

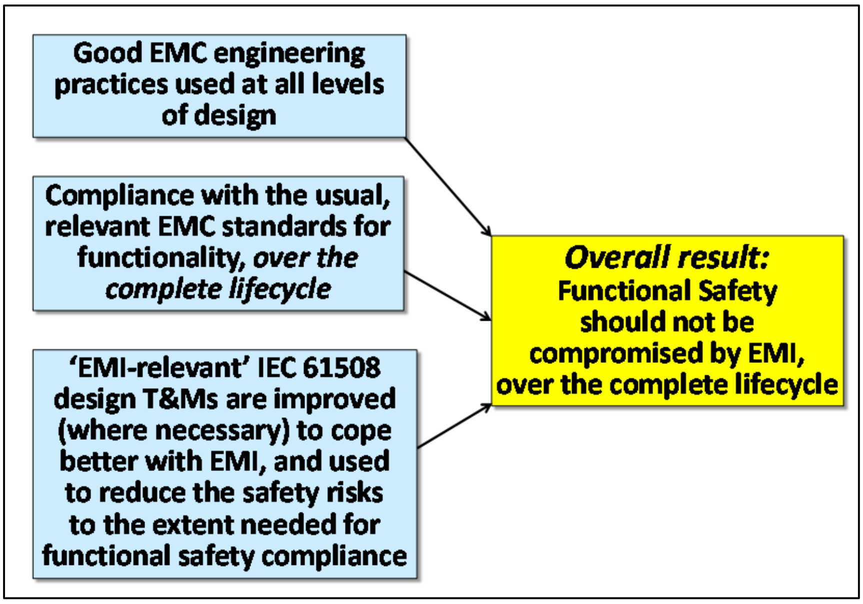
Between 1997 and 2010 I had been assuming that all that was needed to achieve EMC4FS without using big, heavy, costly ‘grey boxes’ (see later) was to become clever enough in EMC design, and in EMC design verification/validation (which include, but could not be limited to, EMC testing).

But no-one had asked me (or anyone else that I knew of) to actually *do* such a project, so my assumptions – and those of the two IEC committees working on standards for EMC4FS – went untested. Then, whilst attending a meeting of The 61508 Society (www.61508.org) I met some companies who had tried to put these assumptions to work, and found they fell short of being in any way practicable.

They eventually made me understand their problems, and – as it happened – chance discussions in recent years with functional safety experts had already primed me with the basic ideas for the alternative, practical approach that was eventually published in August as the IET's 2013 guidance.

Converting my initial ideas in 2010 into something that the IET could publish without gross embarrassment in 2013 [5], required a huge amount of work by members of the IET EMC4FS WG, especially the functional safety experts Barry Lytollis and Brian Kirk. It also required over 160 excellent comments on its first draft from a very wide range of experts in either Functional Safety or EMC.

So, what is this new, alternative and (for the first time ever) practical and cost-effective approach which doesn't require using military-style 'big grey boxes'? It has three parts, as shown in Figure 1.



Good EMC engineering practices used at all levels of design

Compliance with the usual, relevant EMC standards for functionality, *over the complete lifecycle*

'EMI-relevant' IEC 61508 design T&Ms are improved (where necessary) to cope better with EMI, and used to reduce the safety risks to the extent needed for functional safety compliance

Overall result: Functional Safety should not be compromised by EMI, over the complete lifecycle

Figure 1 Overview of the approach taken by the new IET guide

To use this new approach, the EMC community in general has a little more to learn to apply good EMC engineering practices to Functional Safety-related systems, and to equipment that is intended to be used in such systems. It also has a little more to learn to design and construct such systems and equipment with sufficient confidence that they will continue to comply with their relevant EMC test standards throughout their lifecycles.

And designers and independent assessors in the Functional Safety community have a little more to learn too, to apply the techniques and measures (T&Ms) they know very well in slightly different ways to deal correctly with all EMI.

No EMC T&Ms should be relied upon, on their own. The functional safety designer chooses a set of T&Ms which ensure that, regardless of the EM disturbance that causes the error, malfunction or failure, the overall functional safety specifications are met. The lower the level of acceptable functional safety risk, the greater is the amount of work and documentation, and the higher is the competence, required in choosing EMC T&Ms – just as has been the case for 61508's T&Ms since 2000.

The IET's new guidelines [5] can be applied to complete safety-related systems, or to any parts of them, see Figure 2.

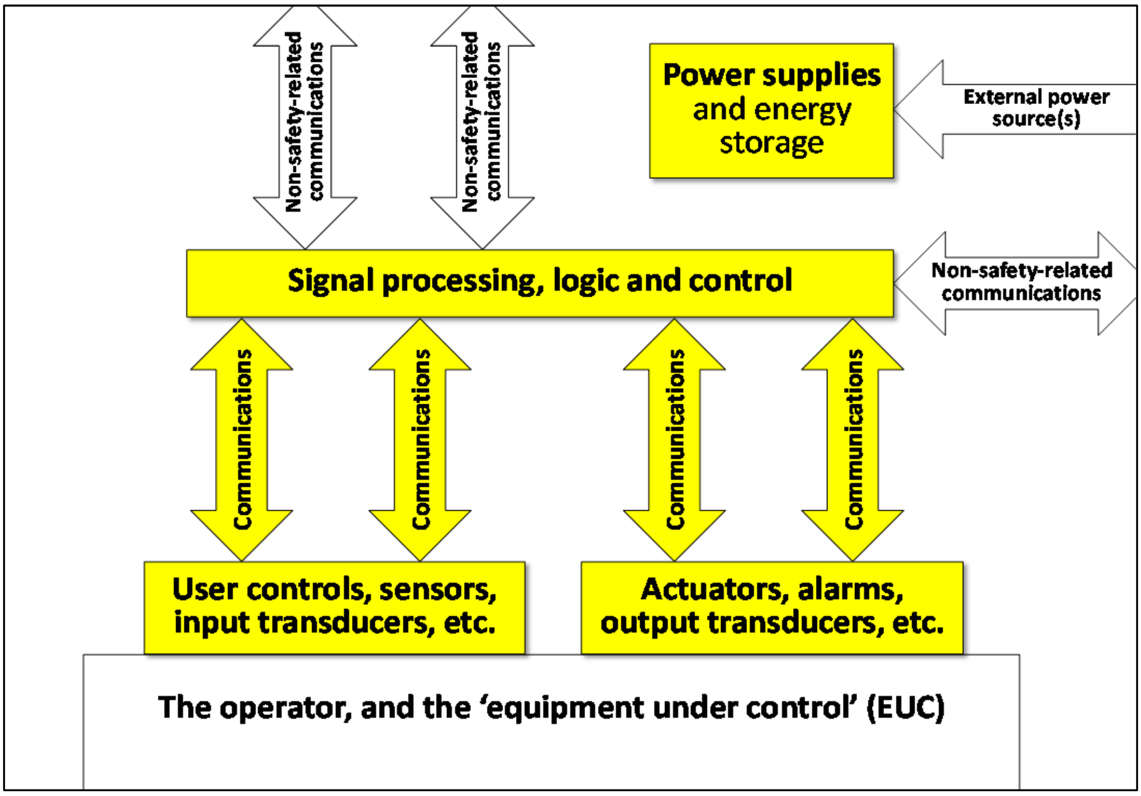

Non-safety-related communications
Non-safety-related communications
Power supplies and energy storage
External power source(s)
Signal processing, logic and control
Non-safety-related communications
Communications
Communications
Communications
Communications
User controls, sensors, input transducers, etc.
Actuators, alarms, output transducers, etc.
The operator, and the 'equipment under control' (EUC)

Figure 2 Overview of a safety related system and its constituent parts (in the yellow boxes)

There is no reason why the traditional 'big grey box' approach (described in Section 2) shouldn't be applied in combination with EMC T&Ms such as those described in the IET's new guide [5]. For example, a complete safety-related system might be constructed from items of equipment supplied by third-parties (custom-designed, batch- or volume-manufactured) some of which use the 'big grey box' method, with the remainder using EMC T&Ms from [5].

Please note: I am an EMC engineer, not a functional safety engineer, and this article is written for EMC engineers – so I hope any functional safety engineers who read it are not *too* appalled by my simplifications and mistakes in matters of functional safety!

2 The 'big grey box' approach

This is a perfectly valid way of achieving EMC4FS that has been used for many decades, and requires no knowledge of the possible EM disturbances (i.e. EM 'threats') that could occur over the entire lifecycle.

It has been used for so long in the military and telecommunication sectors that there are many EMC engineers who are skilled in applying it, and many EMC component manufacturers who can supply appropriate parts for it.

The essential approach is to place the safety-related electronics in a shielded enclosure that provides at least 80dB of shielding effectiveness for both magnetic and electric fields over the entire frequency range (e.g. 20Hz to 26GHz), and is very rugged to withstand physical/climatic environments over its lifecycle without significant degradation in their shielding performance. Such enclosures must be used with similarly rugged 'big grey power filters' and 'big grey power surge suppressors'. Signals enter and exit such boxes through military-style circular connectors fitted with filter/surge suppression pins, shielding, or both. Such enclosures are made of very thick metal plates with seam-welded or conductively gasketted joints, hence the term 'big grey boxes'. Figure 3 shows some examples.

The problem with this 'brute force' approach is that it may be too large, heavy, costly – or even just too ugly – for many modern safety-related systems, especially those made in high-volumes, for example for use in civilian motor vehicles.

Where functional safety designers cannot (or choose not to) apply the ‘big grey box’ method described above, they can now use the IET’s new T&Ms [5].

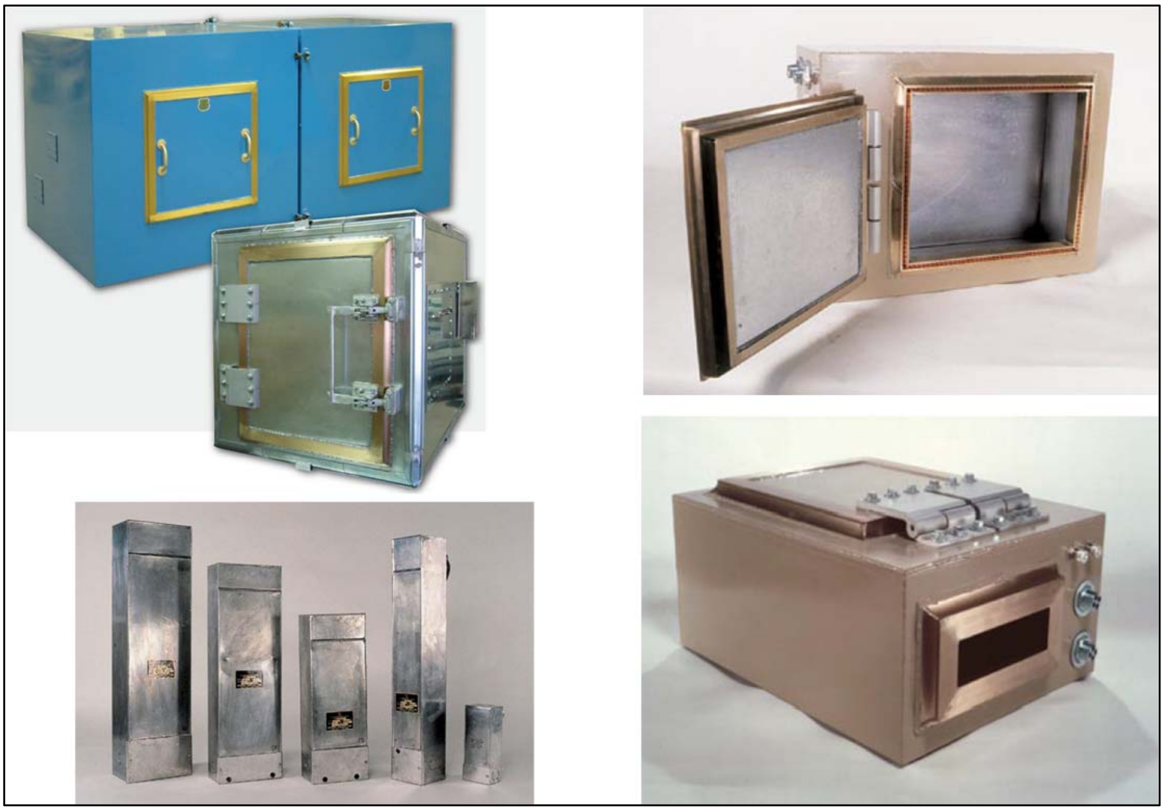


Figure 3 Some examples of big grey boxes and their big grey filters and surge suppressors
(these examples are from Universal Shielding, Inc., but there are several
other manufacturers of such boxes and filters/suppressors)

PS: Can anyone suggest a better name for what I am calling ‘the big grey box’ method?

3 Some more detail on EMC4FS

The basic standard on Functional Safety, IEC 61508 [6], and the standards developed from it, are concerned with ensuring that complex electronic equipment functions in such a way that safety risks remain within acceptable levels. For example, malfunctions in the flight control computers of passenger airliners can result in very high levels of risk (e.g. several hundred people killed).

IEC 61508 and related standards therefore require all reasonably foreseeable errors, malfunctions and faults (including, for example, bad solder joints) over the lifecycle, including those caused by aging, corrosion, accidental or intentional misuse, etc., to be detected and appropriate actions taken to ensure functional safety risks are kept lower than some (previously decided) maximum tolerable level.

(I’m going to use “equipment” throughout this article to mean all types of electronic devices, modules, units, products, sub-systems, systems, installations, etc.)

In practice, the safety-related activities that occur on detecting an error, malfunction or fault in software or hardware fall into two broad categories:

a) Controlling the equipment concerned so that it becomes safe. This is typical of dangerous machinery, for example, by causing it to cease operating, and is called 'putting the equipment under control into a safe state'.

   It is important to note that, except for the availability requirements described later on, safety designers don't care if the equipment is damaged or otherwise made unusable – as long as it remains safe enough.

b) Correcting for the detected error, malfunction or fault so that the equipment continues to operate in a safe manner. This is typical of, for example, life support machinery, which of course doesn't have a 'safe state' – it has to keep working as intended to keep the person alive. This might be achieved, for example, by switching from the malfunctioning control system to a backup system.

   As well as the obvious medical life-support equipment such as ventilators and pacemakers, this category includes rebreather-type diving suits and spacesuits. Most of us don't find ourselves underwater using rebreathers (instead of SCUBA diving gear), or making a spacewalk, but there is another category that has no safe state which almost all of us use daily – passenger transport by road or by air.

   Cars and airliners that are under way have no safe state, they cannot just be powered down like (for example) a production machine, so their safety-related control systems must be of the type that maintains driver or pilot control despite malfunctions and faults. [7] is an example of the safety problems that can arise when this fact is ignored or forgotten.

All electronic equipment can suffer errors, temporary malfunctions or permanent damage due to EMI, and so the ability to withstand EM disturbances is important for achieving acceptable levels of functional safety risk. For this reason, compliance with the IEC's basic publication on EMC4FS, IEC TS 61000-1-2 [8], is now a normative requirement of IEC 61508 [6]. However, there is a problem with this: [8] has the same approach as the IET's 2008 Guide [2] and so requires impractical levels of EMC expertise (if the big grey box' approach is not used).

The 2008 guidance [2] was based on [8], and so both documents base EMC4FS design – and its verification and final (usually independent) validation by an accredited Functional Safety Assessor – on a detailed assessment of the worst-case EM environment over the anticipated lifecycle. Unfortunately, there are large practical difficulties with determining the lifecycle EM environment well enough.

Both [8] and [2] also list numerous T&Ms that may be used for design, verification and validation, but neither provides detailed information on how to make an EMC design comply with a specified level of functional safety risk; or on how an independent functional safety assessor could validate that it had achieved that specification.

In consequence, EMC engineers typically focus on what they know best: using EM mitigation techniques in design (filtering, shielding, surge suppression, galvanic isolation, etc.) and on immunity testing for its verification/validation.

Unfortunately, the design confidence required to achieve acceptable levels of functional safety risks according to [6] is between one and four orders of magnitude greater than most EMC engineers and EMC testers have expertise in achieving. So, although this approach seemed like a good idea when [8] and [2] were written, in practice it has been found to suffer severe difficulties.

It is important to understand that [6], [8] and their related and alternative standards, are *safety* standards, and so are very different from EMC standards. Complying with them requires expertise in achieving functional safety – an engineering discipline developed in total isolation to the discipline of EMC, with which it shares *no* concepts or terminology.

This great difference between the two disciplines adds hugely to the difficulties faced by any EMC or Functional Safety engineers who are expected to ensure that equipment achieves an acceptable level of functional safety risk over its entire lifetime despite all EMI.

As briefly discussed in Section 1, the practical difficulties that have been experienced in attempting to apply [2] and [8] spurred the IET EMC4FS WG to create its new (August 2013) guidance [5].

All EM disturbances that are not sufficiently attenuated by mitigation such as shielding, filtering, surge suppression, etc., result in EMI problems. All such EMI appears as problems with signal, data or power integrity in hardware, software or both, where they can be dealt with by the T&Ms that designers of functional safety-related hardware and software are very familiar with. These T&Ms have (mostly) been listed in [6] since 2000, and are all very well-proven and well-understood through having been developed and used in practice for many years (even decades) before then.

Functional safety designs are always subjected to independent safety assessment, and if the independent assessor doesn't like a design, or thinks the verification and validation it has been subjected to does not prove it is safe enough, he or she has an absolute veto on that design being manufactured. So, independent functional safety assessors are already very familiar with the design T&Ms listed in 61508 [6].

Although these design T&Ms have been found to be quite effective against the effects of EMI on hardware and software, they were not originally developed to deal with EMI and so, as was mentioned in Section 1, the new IET guidance recommends how they may be improved so that a designer may, for the first time, satisfactorily demonstrate to an independent functional safety assessor that errors, malfunctions and faults caused by EMI should not cause functional safety risks to rise above the specified tolerable levels.

For example, a common 61508 T&M is to have two identical sets of hardware and software with the same inputs, and performing the same operations on that data. If an error, malfunction or fault occurs in one of these 'parallel channels', a comparator detects that their outputs no longer agree and triggers appropriate actions to maintain safety.

However, the effects of a given EMI in circuits or software are 'systematic' and not random, so the errors, malfunctions or faults it creates in identical channels can easily be so similar that the comparator cannot tell that there is a problem at all. Such systematic errors are often called 'common-cause', and the IET's new guide recommends that when using parallel channels, one of them should be run on inverted data with respect to the other.

Now the common-cause systematic effects of EMI will have different effects on the data in the two channels, making it very much more likely that the dual-channel technique will detect errors, malfunctions and faults caused by EMI. Note that inverting the data in one channel and re-inverting it back for comparison adds nothing to the cost of manufacture when using FPGAs, as most designers do.

The IET's new guide also recommends that when using parallel channels, they are realized using different architectures for their hardware and their software, which achieve the same end-result. This is an especially valuable technique when using three or more parallel channels with voting to maintain safe operation where there is no safe state, and, for example, this technique is commonly used for the flight control electronics of modern airliners. Often thought of as an expensive 'high-end' technique, when realized in volume-manufactured silicon chips it adds little extra cost.

There is of course a very wide range of safety-related systems, and so the functional safety actions that are triggered by the detection of an error, malfunction or fault can be very different. A 'Safety Case' documents what actions are taken, and how/why they maintain the required level of safety risk, and it is also assessed by the independent functional safety assessor.

4 The concept of Safety Integrity Level (SIL)

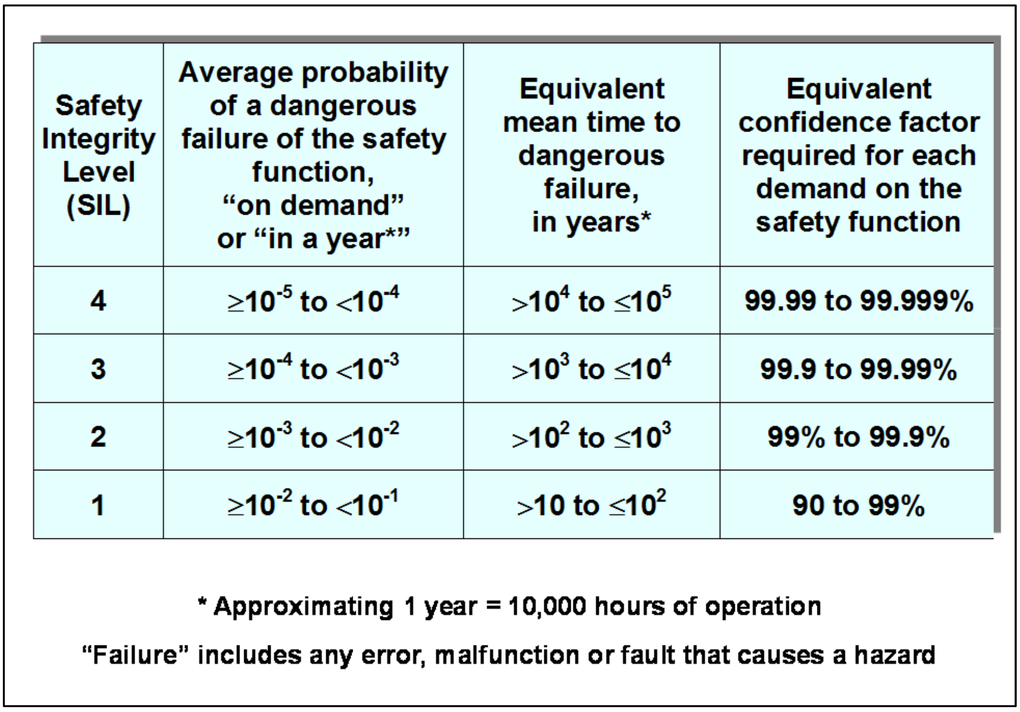
Achieving Functional Safety (i.e. Risk Management) by complying with [6] requires specifying the Safety Integrity Level (SIL) for each of the 'Safety Functions' that a Functional Safety-related system has to perform.

Examples of safety functions include the safe shut-down of a process plant if temperatures or pressures exceed certain limits; stopping a rotating machine if a guard is opened; stopping a robot arm if a person happens to be in its programmed path; switching to a back-up system when the main flight control system in the aircraft fails, etc.

Each safety function is assigned a SIL on the basis of the acceptability of the rate of dangerous failures (i.e. the acceptable level of risk) for what it is intended to control. There are four SILs, each one corresponding to a decade range of rate of dangerous failures, as shown in Figures 4 and 5 (copied from [9], which adapted them from [6]).

An "on demand" safety function is one that only operates when needed, such as an automatic "safe stop" when an industrial machine suffers an excessive overtravel or overspeed.

A "continuous" safety function is one that is operating all the time, such as the "safe torque" generated by a motor drive when people are working directly on its driven equipment and are exposed to hazards such as cutting, crushing, etc.



Safety Integrity Level (SIL)	Average probability of a dangerous failure of the safety function, "on demand" or "in a year*"	Equivalent mean time to dangerous failure, in years*	Equivalent confidence factor required for each demand on the safety function
4	$\geq 10^{-5}$ to $< 10^{-4}$	$> 10^{4}$ to $\leq 10^{5}$	99.99 to 99.999%
3	$\geq 10^{-4}$ to $< 10^{-3}$	$> 10^{3}$ to $\leq 10^{4}$	99.9 to 99.99%
2	$\geq 10^{-3}$ to $< 10^{-2}$	$> 10^{2}$ to $\leq 10^{3}$	99% to 99.9%
1	$\geq 10^{-2}$ to $< 10^{-1}$	> 10 to $\leq 10^{2}$	90 to 99%

* Approximating 1 year = 10,000 hours of operation

"Failure" includes any error, malfunction or fault that causes a hazard

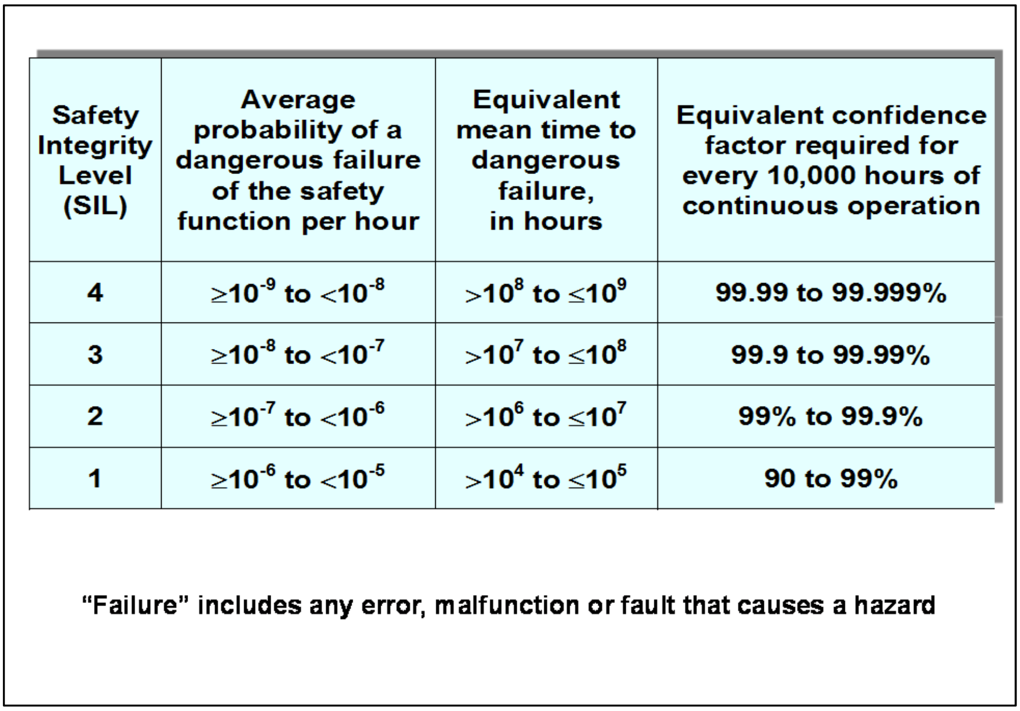
Figure 4 Design confidence requirements for "on demand" safety functions

SIL4 is associated with the lowest rates of dangerous failure (lowest levels of acceptable risk), and so requires the highest confidence, in both the functional safety design and its independent validation. Typically, SIL4 is used for electronic systems for aircraft flight controls; railway signalling; nuclear plant safety shut-downs, and the like.

SIL3 permits a ten times higher rate of dangerous failures than SIL4 (a ten times higher range of acceptable risk), and so requires a ten times lower range of design/validation confidence. SIL3 is often applied to equipment manufactured in medium/high volumes, for example: automobile driving control systems (throttle, brake, steering, etc.); machinery; process control, etc., where the consequences of failure are serious, but not as serious as SIL4.

At the other end of the scale, SIL1 is used for systems that need to be just that little bit safer than is usually achieved by applying normal good design and verification practices.

Another way of looking at SILs, is to consider that SIL1 requires the levels of risk achieved by the usual good design and their verification/validation practices to be reduced tenfold; SIL2 requires risk levels to be reduced 100-fold; SIL3 requires a risk-reduction of 1000-fold, and SIL4 requires a risk reduction of 10,000-fold, i.e. to 1/10,000th or 0.01% of the risk level achieved by normal good engineering practices.



Safety Integrity Level (SIL)	Average probability of a dangerous failure of the safety function per hour	Equivalent mean time to dangerous failure, in hours	Equivalent confidence factor required for every 10,000 hours of continuous operation
4	$\geq 10^{-9}$ to $<10^{-8}$	$>10^{8}$ to $\leq 10^{9}$	99.99 to 99.999%
3	$\geq 10^{-8}$ to $<10^{-7}$	$>10^{7}$ to $\leq 10^{8}$	99.9 to 99.99%
2	$\geq 10^{-7}$ to $<10^{-6}$	$>10^{6}$ to $\leq 10^{7}$	99% to 99.9%
1	$\geq 10^{-6}$ to $<10^{-5}$	$>10^{4}$ to $\leq 10^{5}$	90 to 99%

"Failure" includes any error, malfunction or fault that causes a hazard

Figure 5 Design confidence requirements for "continuous" safety functions

EMI is identified in [6] and [8] as a 'Systematic Failure Mode', meaning that it is not statistically random, but instead is a feature of a given design, in the same way that software "bugs" are considered to be a feature of a given software design, rather than occurring at random.

The SIL concept applies to the operation of a completed safety-related system, which may use not just electronic, but also electro-mechanical, mechanical, building works (e.g. blast shields) and personnel management (e.g. restricting access to the area inside the blast shields). Typically, I am told, the EMI contribution to any SIL is no more than 10% of the total risk. So the numbers in Figures 4 and 5 for the various SILs need to be reduced at least ten-fold when considering the EMC design confidence alone.

Systematic failures (including: errors; recoverable malfunctions, and permanent faults) can only be dealt with by the use of well-proven design techniques, plus well-proven verification and validation techniques. Together, these must achieve the confidence in the design, and in its (usually independent) validation, that is required by the SIL specified for the safety function concerned.

Trying to anticipate the rates of occurrence of EM disturbances is generally inappropriate when trying to achieve a specified SIL. For example, even if an especially extreme EM disturbance happened only once every ten years on average, the SIL corresponds to the level of confidence that the safety function will withstand this rare EM event without failing *whenever it happens*.

This is an important aspect of risk management that is often misunderstood. I often see EMC engineers incorrectly attempting to achieve SILs (or ASILs, as used by ISO 26262) by using statistical reasoning for the rate of occurrence of EM disturbances. It is not unimportant that, by removing EMC experts from the need to understand anything at all about functional safety engineering, [5] helps to avoid dangerous mistakes caused by misunderstandings.

5 Practical difficulties in determining the worst-case EM environment(s)

[6] requires safety-related equipment to be designed, and for its design to be verified and validated, to cope with the worst-cases of all its environmental exposures over its anticipated lifetime. For this reason, [8] and [2] require EMC design and verification/validation to be based upon an accurate determination of the worst-case EM environment(s) that could be experienced over the anticipated lifetime. Unfortunately, there are significant practical difficulties in doing this.

Most industries have only very general guidelines on EM environments to follow, such as IEC 61000-2-5 [10] and the IEC 61000-4 series of immunity testing standards [11]. These are based on so-called "economic/technical compromises" that ignore any considerations of safety-related or other risk-managed applications. Depending on which standards team members one talks to, the types and levels of the EM disturbances in these documents are estimated to cover between 80% and 95% of what can be expected in "normal" EM environments.

Worst-case (i.e. most extreme), rare or unusual EM disturbances are very important indeed when trying to improve the normal immunity to EMI by, say, 10,000 times for a safety function preventing a vehicle's speed from going out of driver control – but are not considered at all in [10] or [11].

Many manufacturers of safety-related systems, and independent functional safety assessors, have told me that they cannot even begin to comply with [8], because they have no expertise in assessing worst-case EM environments over the anticipated lifetime of their equipment, and cannot afford to employ such expertise.

There are also significant problems concerning the ability of anyone to predict what the worst-case EM environment will be for a given location, number of locations, or vehicle route over the next 10, 20, 30 or more years (for example, railway trains are currently being designed for a service life exceeding 50 years).

Military and aerospace EMC designers have the big advantage that a lot of work has gone into (and is still going into) characterizing their EM environments and their corresponding immunity tests, having regard to mission-criticality. However, even they might balk at predicting their critical systems' EM environments 30 or 40 years hence, or assessing the possibilities for any of the foreseeable EM disturbances to happen simultaneously or in some time-sequence that is critical for the equipment concerned (see [12] and [13]).

A very big advantage of [5] over the lifecycle EM environment assessment required by [2] and [8], is that its T&Ms ensure that the required design confidence for the specified SIL is achieved as regards any/all EM disturbances.

Because they cover all signal/data/power integrity issues, they also cover all EMI, even from EM disturbances and combinations of them which were unforeseen, or even unforeseeable, and so they cope with any/all possible future changes to the EM environment.

6 Practical Difficulties with EM mitigation

EMC designers who use the 'big grey box' approach described in Section 2, can provide evidence – usually obtained from the suppliers of their big grey boxes, big grey filters and big grey surge suppressors – that satisfies independent functional safety assessors that the design of their EM mitigation is so comprehensive and reliable that all risks due to EM disturbances would be low-enough for the chosen SIL over the anticipated lifecycle. However, as I said earlier, such "brute force" EM mitigation approaches are usually too large, heavy, costly or ugly for volume-manufactured safety-related systems, or equipment intended for use in them.

Filters made from chokes and capacitors, and shielding, suffer from resonant frequencies at which they provide *gain* rather than attenuation. Filter resonances are affected by their real-life source and load impedances – and are not tested by standard EMC tests.

Shield resonances are affected by the size of the gaps at their inevitable joints and seams, no matter how narrow those gaps are (the film of oxide that naturally forms on plain aluminium is more than sufficient to create a resonant aperture).

A knowledgeable EMC designer will ensure that these resonances occur at frequencies outside those at which there could be any reasonably foreseeable threats in the EM environment(s) over the lifetime. But component values can change over time, due to internal degradations and/or temperature, and soldered joints and other kinds of electrical connections can also degrade or fail over time, for example due to shock, vibration, galvanic corrosion, etc. For example, some low-cost X2 capacitors fully compliant with the relevant IEC standard lose 10% of their value for every 1000 hours of operation!

The result is that filter and shield resonant frequencies will change over time, generally in the wrong directions, and can cause gain (or at least, insufficient attenuation) in the frequency ranges where significant EM threats can occur in the EM environment.

Using two or more different types of filters or shields in a redundant combination makes it possible to mitigate the effects of such resonance shifts, but interactions between the multiple filters or shields adds additional possibilities for resonances to arise, and so they must also be dealt with.

[5] avoids this whole problem, by making it practical to deal with most/all the effects of EMI in the design of the circuits and software, so that EMC expertise is rarely needed.

7 Practical difficulties with verifying and validating the SIL of an EMC design

[9] [14] [15] [16] and [17] show that any affordable immunity test plan is unlikely, on its own, to provide sufficient confidence in design verification or validation, even for SIL1, for reasons far too numerous to list here.

[12] and [13] discuss ways of extending the "coverage" of immunity tests, perhaps even to the point of being able to prove compliance with SIL1, *for new equipment assembled correctly with nominal components*. But such testing would still leave uncontrolled the important EMC issues of (for example): component tolerances, degradations, bad batches and counterfeits; assembly errors; ageing, corrosion, foreseeable faults, use and misuse, etc.

IEC 61508 [6] has always understood that very few aspects of a functional safety design can be completely verified or validated for compliance with the specified SIL by using testing techniques alone, and this applies to testing EM immunity just as much as it does to testing software for bugs.

To achieve design verification/validation with the confidence levels required by the SILs, [6] [8] and [2] specify the use of a wide variety of design assessment T&Ms, including, for example:

- Demonstrations
- Checklists
- Inspections
- Expert Reviews and Assessments
- Audits
- "Walk-Throughs"
- Validated computer modelling, simulation, etc.
- Testing (which cannot be sufficient on its own)

The new guidance in [5] avoids this whole problem area, by moving most of the EMI risk management issues to the choice of appropriate hardware and software design T&Ms, in which most independent Functional Safety assessors have developed considerable expertise since [6] was first published in 2000, if not earlier.

8 The ‘T&M’ solution to the above practical difficulties

Hardware and software design T&Ms have been developed over at least two decades specifically to deal with all reasonably foreseeable degradations and faults, as well as software bugs. As I said in the introduction, these were never intended to deal with EMI, and yet many of them are very good at doing just this and the new IET guidance [5] extends their application specifically to cover all of the errors, temporary/intermittent malfunctions and permanent failures that could be caused by EMI.

Depending on the thoroughness with which the new IET Guide’s T&Ms are applied, the confidence in withstanding EM disturbances can be increased by 100-fold to help achieve SIL1, or up to 100,000-fold to help achieve SIL4, as discussed above.

The key issue in understanding the approach in [5], is that the effect of EMI on electronic hardware and software is *always* a degradation of, or temporary or permanent damage to, signal/data integrity (SI) and/or to power integrity (PI). SI and PI degradations and failures can *always* be dealt with by applying appropriate techniques (including error detection and/or correction) in the design of the hardware, software and DC power supplies.

Where equipment has a ‘safe state’ (e.g. powered down), *error detection* T&Ms can be used to control putting it into that safe state (e.g. by switching it off, in some applications) whenever they detect an error, malfunction or failure.

Where there is no safe state, *error correction* techniques can be used to restore the correct signals, data processing and power rails, so that the equipment continues to work as intended by its designers. In some circumstances where continuous full-specification operation is necessary, EMC expertise in preventing permanent damage from overvoltages, overcurrents or excessive power dissipations may be required. Such EMC requirements should be specified by the hardware or software functional safety experts.

Most of the ‘design hardening’ T&Ms described in [5] have been listed in [6] since 2000, and so are very familiar to the designers of functional safety-related equipment, and their independent assessors. The few T&Ms in [5] not already listed in [6] are mostly well-established good practices in functional safety engineering, and so are also familiar to designers and their assessors. However, there are one or two T&Ms in [5] that are completely new, but they should not cause any difficulties for designers or assessors.

The knowledge that permits these well-proven ‘hardening’ T&Ms, which are already used for compliance with [6] and its related standards, to be extended to cover EMI for the specified SIL, is that EMI can cause:

- a nearly infinite variety of degraded, distorted, delayed, altered-priority, false, etc., signals/controls/data *at one or more* of the system’s ports (including the enclosure port);
- *plus* under/overvoltages, intermittencies, interruptions, noise or even permanent damage *on one or more* of its signal/control/data lines and DC power rails;
- any/all of the above occurring simultaneously or in any time-sequence.

What this means in practice is that the new IET guide’s hardware and software T&Ms will generally need to be applied more rigorously than has been typical for the regular T&Ms listed in [6].

9 The great importance of ‘availability’

I have heard of a new railway signalling system that was designed without any EM mitigation. It had a safe state: when its signal was at red, a train on that line may not proceed beyond that signal. All its EMC immunity and other design verification and validation techniques proved that whatever errors, malfunctions or failures arose in the electronic hardware or software, the signals always failed to red, which the rail industry calls a “right-side failure” (RSF).

But when the system was deployed on an actual railway, about every 30 seconds EMI caused by its normal EM environment would make it fail to its safe state (red light, RSF) – and no trains could run. The signalling system was perfectly safe – unfortunately it made the railway inoperable by stopping *all* of the trains, *all* of the time!

Equipment that “fails safe” too often can be expected to suffer unauthorized modifications to reduce its downtime, for example by disconnection of its safety-related systems, in an attempt to improve availability and improve productivity. Manufacturers who fail to take this into account are at increased risk of liability under Product Liability legislation, at least in Europe.

Because, therefore, it is necessary to maintain low levels of downtime, [5] recommends passing tests to the relevant emissions and immunity standards for the application and its normal EM environment. These standards may be those required for compliance with the EMC Directive, or they may be customer-specified EMC standards (typical of military, underground railway, and automotive applications, for example).

This is, of course, what is already done at the moment – except that this level of EMC performance needs to be maintained over the entire lifecycle.

To ensure that equipment continues to be compliant with its relevant EMC standards over its lifecycle, some manufacturers take equipment that complies with its usual EMC emissions and immunity test standards, artificially age it using well-established acceleration techniques, then retest the aged units to check that they still comply with those EMC standards.

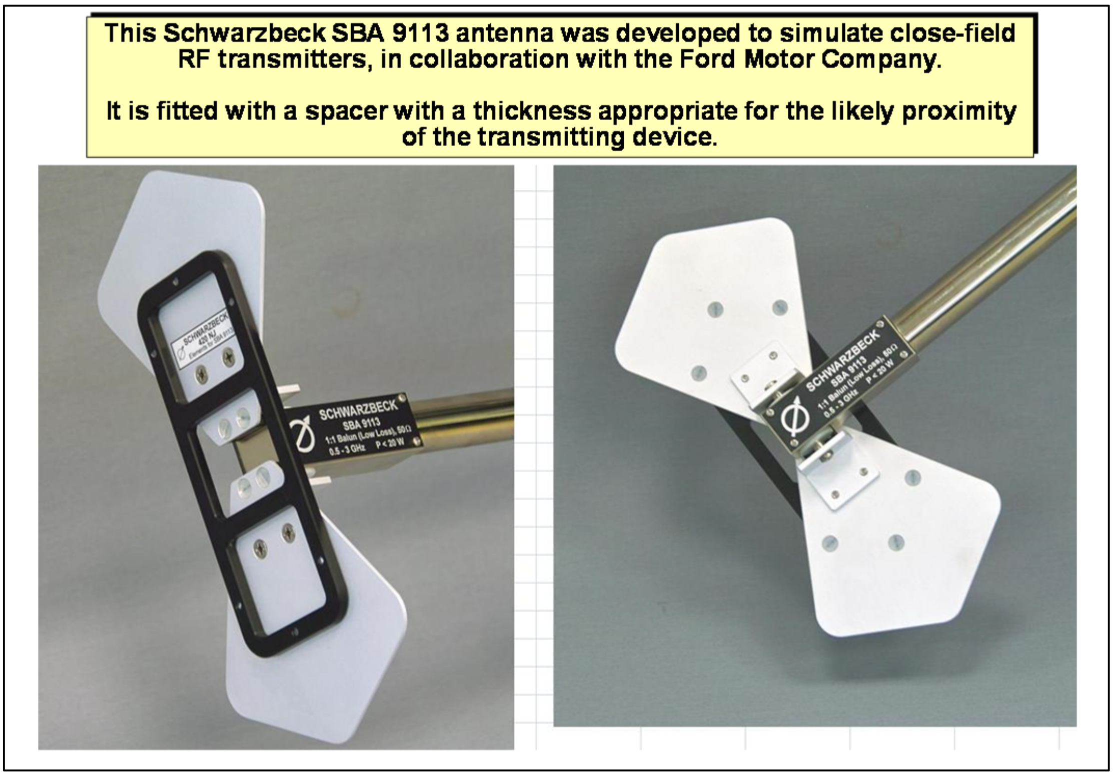
Another approach, sometimes used in large installations or costly military vehicles, is to inspect and/or test all of the EM mitigation measures at regular intervals during their lifecycles, refurbishing or replacing anything that is found to have degraded significantly or is close to its individual, planned, end-of-life. (There is at least one manufacturer of equipment designed for in-situ testing whether filters and surge suppressors have degraded unacceptably and need replacing.)

Although I said a few minutes ago that passing tests to the relevant emissions and immunity standards for the application and its normal EM environment is what is already done at the moment, this is not quite correct. For example, most EM environments now contain close-proximity radio transmitters, such as cellphones, datacomm’s that use the cellphone networks (e.g. M2M [18]), Bluetooth earpieces, Wi-Fi, etc. but the existing immunity standards do not cover this situation.

Indeed many modern work environments (including healthcare) actually now <u>rely</u> on the close proximity of radio transmitters! Testing using the usual far-field RF immunity tests such as IEC 61000-4-3 cannot simulate close-field RF transmitters, so – where close-proximity radio transmitters cannot be reliably kept away from the safety-related system – it should comply with [19].

Locations that are exposed to radar pulses from airports, harbours, military airbases, naval bases, weather radars, etc., might need to apply the immunity test [20].

In general, for reasons of maintaining appropriate levels of availability, wherever an EM environment suffers from significant levels of EM disturbances that might cause unacceptable downtime when the EMI they cause triggers the operation of a safety-related system, safety-related systems should be designed and tested to ensure that they complies with the relevant immunity test standards over their lifecycles.



This Schwarzbeck SBA 9113 antenna was developed to simulate close-field RF transmitters, in collaboration with the Ford Motor Company.

It is fitted with a spacer with a thickness appropriate for the likely proximity of the transmitting device.

Figure 6 The antenna used when testing to [19] for close-proximity radio transmitters

10 Some final words

Previous guidance in [8] and [2] on managing functional safety risks assumed the use of very high levels of EMC expertise to accurately determine worst-case EM environments, and to improve the effectiveness of EMC design by between 100 and 100,000 times more than is normally achieved – over the entire lifetime of an equipment, not just when it is new.

The lack of such EMC expertise, and the apparent lack of any interest in obtaining such EMC expertise, plus the many practical difficulties associated with this EMC-engineering-based approach, are currently preventing EMI from being taken fully into account in functional safety-related systems (unless they are using the 'big grey box' approach).

Indeed, it seems very unlikely that the approach assumed by [8] and [2] could ever be made to work in practice, even if the assumed EMC expertise magically became available.

For these reasons, the latest guidance from the IET's Working Group on EMC4FS [5] avoids any need to develop or employ greater EMC expertise than is necessary to ensure compliance with the relevant emissions and immunity test standards over the lifecycle.

It does this by moving part of the work onto the existing base of experienced hardware and software functional safety designers, and their experienced independent functional safety assessors.

[5] makes it practical and cost-effective for this community of designers and assessors to manage functional safety risks as regards EMI, by extending the use of their existing, well-proven and well-understood "design hardening" T&Ms in both hardware and software.

The effects of EM disturbances that exceed what can be coped with by compliance with the relevant immunity test standards, will be detected by the hardware and software T&Ms and appropriate actions taken to maintain the functional safety risks at acceptable levels, according to the safety case.

11 References

[1] K. Armstrong, “New Guidance on EMC-Related Functional Safety”, IEEE 2001 International EMC Symposium, Montreal, August 13-17, ISBN 0-7803-6569-0.

[2] The IET, “EMC for Functional Safety”, Edition 1, Aug. 2008, from www.theiet.org/factfiles/emc/emc-factfile.cfm, or www.emcacademy.org/books.asp

[3] K. Armstrong, “The New IET guide – how to do EMC to help Achieve Functional Safety. In: C. Dale, T. Anderson (ed’s) “Making Systems Safer”, Proceedings of the 18th Safety-Critical Systems Symposium, Bristol, UK, 9-11 February 2010. Published by Springer, London, in 2010, ISBN: 978-1-84996-085-4.

[4] K. Armstrong, “The IET’s new guide: EMC for Functional Safety — Applying Risk Management to EMC”, Inside Functional Safety, Vol. 2010, Iss. 02, www.insidefunctionalsafety.com/article/29.html

[5] The IET, “Overview of techniques and measures related to EMC and Functional Safety”, August 2013. This PDF document can be downloaded from the list at www.theiet.org/factfiles/emc/index.cfm, or downloaded directly from www.theiet.org/factfiles/emc/emc-overview.cfm.

[6] IEC 61508 Ed.2:2010, (in seven parts), “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems”, IEC basic safety publication.

[7] Melissa Fyfe and Grace Dobell, “Outcry on safety forces VW recall”, The Age, Sydney, Australia, June 12, 2013, www.theage.com.au/drive/motor-news/outcry-on-safety-forces-vw-recall-20130611-2o28i.html

All IEC publications may be purchased from http://webstore.iec.ch.

[8] IEC TS 61000-1-2, Ed.2.0, 2008-11, “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”, IEC basic safety publication.

[9] K. Armstrong, “Including EMC in Risk Assessments”, IEEE 2010 International EMC Symposium, July 25-30, Fort Lauderdale, FL, ISBN: 978-1-4244-6307-7

[10] 61000-2-5,“Electromagnetic compatibility (EMC) – Part 2-5: Environment – Description and classification of electromagnetic environments”

[11] 61000-4-x, “Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques”. There are very many parts in this series.

[12] W. Grommes and K. Armstrong, “Developing Immunity Testing to Cover Intermodulation”, IEEE 2011 International EMC Symposium, Long Beach, CA, August 15-19, ISBN: 978-1-45770810-7

[13] K. Armstrong, “Testing for immunity to simultaneous disturbances and similar issues for risk managing EMC”, IEEE 2012 International EMC Symposium, Pittsburgh, PA, August 5-10, ISBN: 978-1-4673-2059-7.

[14] K. Armstrong, “Why Increasing Immunity Test Levels is Not Sufficient for High-Reliability and Critical Equipment”, IEEE 2009 I International EMC Symposium, Austin, TX, August 17-21, ISBN: 978-1-4244-4285-0

[15] K. Armstrong, “Why EMC Immunity Testing is Inadequate for Functional Safety”, 2004 IEEE International EMC Symposium, Santa Clara, CA, Aug. 9-13, ISBN 0-7803-8443-1

[16] W. Radasky, J. Delaballe and K. Armstrong, “7b) Testing EM for Safety”, part of the “Workshop on EMC & Functional Safety”, IEEE 2009 International Symposium on Product Safety, October 26-28, Toronto, Canada

[17] K. Armstrong, “Including EMI in Functional Safety Risk Assessments”, 20th Safety-Critical Systems Symposium, Bristol, UK, 7-9 February 2012, Proceedings: “Achieving Systems Safety”, editors Chris Dale, Tom Anderson, Springer 2012, ISBN: 978-1-4471-2493-1.

[18] Machine-to-Machine communications (‘M2M’), see http://en.wikipedia.org/wiki/Machine_to_machine

[19] It was hoped that this would be addressed by the future IEC 61000-4-39 “Measuring methods for radiation sources in close proximity” , 9kHz to 6GHz, but at the time of writing (January 2016) this standard does not cover this type of electromagnetic disturbance, so the best is to apply ISO 11452-9.2 “Road vehicles — Component test methods for electrical disturbances from narrowband radiated electromagnetic energy — Part 9: Portable transmitters” – or the test method that it is based upon: the Ford Motor Company’s Test Method RI 115 “RF Immunity to hand portable transmitters” in their EMC-CS-2009.1, “EMC Specification for Electrical/Electronic Components and Subsystems”. Many EMC test labs around the world are equipped for, and familiar with doing this test, which can be downloaded from www.fordemc.com/docs/download/EMC_CS_2009rev1.pdf.

[20] RI 114 “RF Immunity 400MHz – 3,100MHz” from Ford Motor company’s EMC-CS-2009.1, “EMC Specification for Electrical/Electronic Components and Subsystems”. Many EMC test labs around the world are equipped for, and familiar with doing this ‘radar’ test, which can be downloaded from www.fordemc.com/docs/download/EMC_CS_2009rev1.pdf.