Risks caused by Electromagnetic Interference



Keith Armstrong and Davy Pissoort continue their discussion on the challenges in managing Functional Safety Risks posed by Electromagnetic Interference (EMI) and present current best practices in techniques and measures to manage the risks posed by EMI.

As introduced in the previous article, Electromagnetic interference (EMI) is what we call any errors, malfunctions or failures in electronics that are caused by Electromagnetic (EM) disturbances such as those listed below. Because all electronics can suffer EMI, it should be taken fully into account when complying with Functional Safety requirements.

Conducted low frequency phenomena	Harmonics, interharmonics Signalling voltages Voltage fluctuations Voltage dips and interruptions Voltage unbalance Power frequency variations Induced low frequency voltages d.c. in a.c. networks
Radiated low frequency field phenomena	Magnetic fields [a] Electrical fields
Conducted high frequency phenomena	Directly coupled or induced continuous voltages or currents Unidirectional transients [b] Oscillatory transients [b]
Radiated high frequency field phenomena	Magnetic fields Electrical fields Electromagnetic fields – continuous waves – transients [c]
Electrostatic discharge phenomena (ESD)	Human and machine
Phenomena of conducted and radiated HPEM environment [d]	
High altitude electromagnetic pulse (HEMP) [d]	

[a] Continuous or transients.

[b] Single or repetitive (bursts).

[c] Single or repetitive.

[d] To be considered in case of special conditions (see IEC 61000-2-13).

NOTE There is no abrupt change between the low frequency domain and the high frequency domain but a soft transition between 9 kHz and 150 kHz. For formal applications the limit is set at 9 kHz (scope of CISPR).

We understand that it is commonplace for Functional Safety projects to allocate one-tenth of the maximum acceptable risk level to EMI, unless there are specific reasons for choosing a different proportion. For example, if a Safety Related system (SRS) is required to maintain a risk of death of 1 in a million per person per year, then the risk of death arising from EMI effects must be less than one in ten million per person per year.

Immunity testing in an Electromagnetic Compatibility (EMC) laboratory is the traditional method of ensuring that EMI is sufficiently unlikely to occur during real life operation, and where safety risks are involved, it has been usual to apply the standard immunity tests at higher levels than otherwise. Although it is now more than 13 years since this approach was publicly revealed as being insufficient [1] [2], it is still used, and this continues to expose people to uncontrolled safety risks, and exposes manufacturers to uncontrolled financial and reputational risks. This is especially so because more advanced electronic systems are increasingly being used to control dangerous activities (e.g. remote-controlled surgical robots; care-giving robots; self-flying goods-delivery drones; autonomous cars, etc.).

"More advanced electronic systems are increasingly being used to control dangerous activities (e.g. remote-controlled surgical robots; care-giving robots; self-flying goods-delivery drones; autonomous cars)"

There is a simple reason why immunity testing is insufficient in proving that EM disturbances should not cause unacceptable levels of functional safety risks: it is physically impossible to test all of the possible states of a modern, programmable SRS.

Even if it *was* possible to test all possible digital states (*which it isn't*), there are additional cost and time barriers to relying solely on immunity testing (discussed in detail in [3]). This makes it obvious that attempting to use immunity testing alone to prove that functional safety risks due to EMI would remain low-enough throughout a lifecycle would cause an 'explosion' in the cost and duration of an EMC test plan [3] [1].

'High-spec', well-maintained EM mitigation (shielding, filtering, surge protection, galvanic isolation, etc.) has long been the traditional military method for reducing risks that could be caused by foreseeable EM disturbances over a lifecycle. Some examples are shown in the figure. It reduces the levels of EM disturbances to which the electronics are exposed to such low levels that EMI cannot occur. Such mitigation is ruggedized so as to maintain its high EM specifications between maintenance and/or refurbishment periods and is over-engineered to cope with the uncertainties in predicting the EM disturbances that could arise.

The large size, weight and/or cost of the ruggedized 'high-spec' EM mitigation approach does not suit many modern SRSs, so the IET's Working Group on EMC for Functional Safety developed a practical alternative based on the expertise that existed in both the EMC and Functional Safety professional communities. After considerable input from a large number of these experts in the UK, the IET first published this guidance in August 2013 [4].



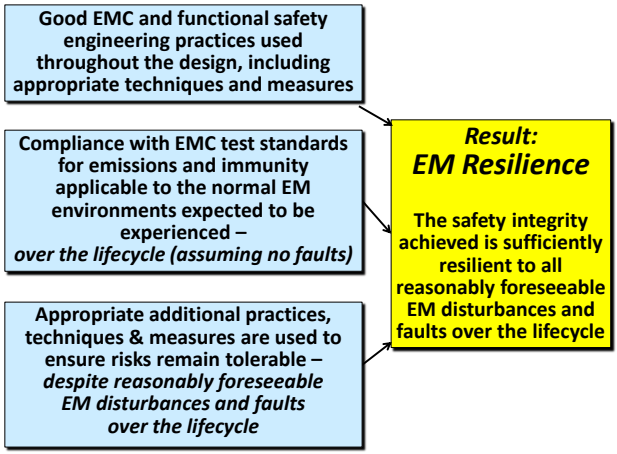
Since then, the IET's WG has revised this guidance, put it through two international commenting rounds and published the result in 2017 as the IET's 'Code of Practice on EM Resilience' [5]. The figure on the next page provides an overview of this 'EM Resilience' approach, which essentially means that the hardware and software could suffer from EMI without causing unacceptable levels of risk.

The draft new IEEE Standard 1848 [6] is a direct development of [5].

IEC 61508 describes many Techniques and Measures (T&Ms) for use in specification, design, verification and validation; for hardware, software and systems. Firstly, to try to prevent avoid errors, malfunctions and faults from occurring, and secondly to reduce any remaining risks to conform to the specified risk levels.

These T&Ms operate on the data and other signals (analogue, digital, etc.) and/or on the electrical power supplies (AC, DC, etc.), but they were never intended to deal with EMI. However, EMI can only affect data, signals and/or power supplies, so it is commonly found that correct application of IEC 61508's T&Ms is very effective in dealing with the effects of EMI. Functional safety designers and their assessors have become very experienced in the use of these T&Ms.

The IET's 2017 guidance [5] provides guidance on how best to apply IEC 61000-1-2:2016 in practice. It details which of IEC 61508's T&Ms are good for dealing with EMI, as well as how to improve their benefits for EM resilience, and includes a few new T&Ms specifically for dealing with the effects of EMI. These modifications do not require functional safety designers or their assessors to learn very much more beyond their knowledge of the existing standards.



EM Resilience T&Ms in design

Electronic hardware, software and system designers are generally familiar with many of these T&Ms, because most of them have been in use for decades.

T&Ms for Redundancy and Diversity include:

- Multiple sensors sensing the same parameters
- Multiple communications carrying the same data
- Storing multiple copies of data
- Processing the same data with multiple processors
- Detecting errors by comparing one value with another, out of any multiple of values
- Correcting errors, for example by 'voting' any two that agree out of three, or three out of five, etc.

All the above benefit from using a wide range of diverse technologies and techniques among their multiple "channels" to improve their effectiveness against the common-cause failures typically caused by EMI. For example, in a system consisting of two identical channels, the signals or data in one channel could be inverted thereby making EMI more likely to be detected when comparing the difference between their outputs, at no extra cost.

T&Ms for Error Detection & Correction include:

- Error detection coding (EDC)
- Error correction coding (ECC)
- Static self-testing checks the hardware and software before operation, preventing start-up if necessary

- Dynamic self-testing checks that the operation of the hardware and software is correct during operation, for example by regularly inputting fixed, known signals/data and checking that the resulting outputs are within the required boundaries. Critical aspects of data processing might be checked for correct operation once every second, or perhaps even more often.

T&Ms for Power Supplies include:

- Window comparators check that power supplies are within design limits.
- Stored energy (e.g. batteries, supercapacitors) used when external power supplies are outside design limits. This is a very common technique used in modern portable devices, such as cell phones or tablet PCs, and the technology is very well-developed as a result.
- Multiple power sources (whether external or internal storage) operated in parallel (e.g., so-called N+1 redundancy) so that the failure of one or more power sources still allows normal operation to continue.
- Before all the available sources of power fail, the system switches to a safe state (if it has one). If it doesn't have one, more energy storage or more redundancy in external supplies is added until the possibility of dangerous failure is as low as required.

Choosing T&Ms for EM Resilience will generally discover that many of the necessary T&Ms have already been chosen for other Functional Safety reasons. However, many of these will need to be modified as described in [5] to optimise their benefits for EM Resilience. Other EM Resilience T&Ms may then need to be added to achieve EM Resilience overall.

In a system, some items of equipment or elements may rely on military-style high-spec mitigation; whilst other may rely on EM Resilience T&Ms.

It is possible to create functionally safe systems by relying solely on IEC 61508's design T&Ms to detect failures and switch the Equipment Under Control (EUC) into a safe state. However, EMI can make them fail to start up, or switch to their safe states much too frequently.

Such systems should be expected to be modified by their users or owners to improve their 'availability' (reduce their downtime) usually by disabling their SRSs, see sections 3.8 and 3.10 in [7]. In the EU at least, product liability laws would seem to categorize such unauthorized modifications as 'foreseeable misuse', making it the *manufacturer's* fault if any deaths, injuries or financial losses resulted from users disabling SRSs to improve an EUC's availability.

As far as EMI is concerned, adequate availability simply requires compliance with the normal relevant EMC immunity test standards. These include immunity test standards that have been used for decades for compliance with the EMC Directive, and customers' EMC specifications for railway signalling, automobiles, military equipment, avionics, etc.

The EMC testing community has extensive experience with ensuring that equipment passes EMC tests when it is shiny and new. The IET's 2017 guide [5] recommends that SRSs maintain their ability to pass all relevant EMC tests *throughout their entire lifecycles.* This should not require competent EMC designers to have to learn a great deal more.

T&Ms for verification and validation

Suitable verification and validation methods include (but are not limited to):

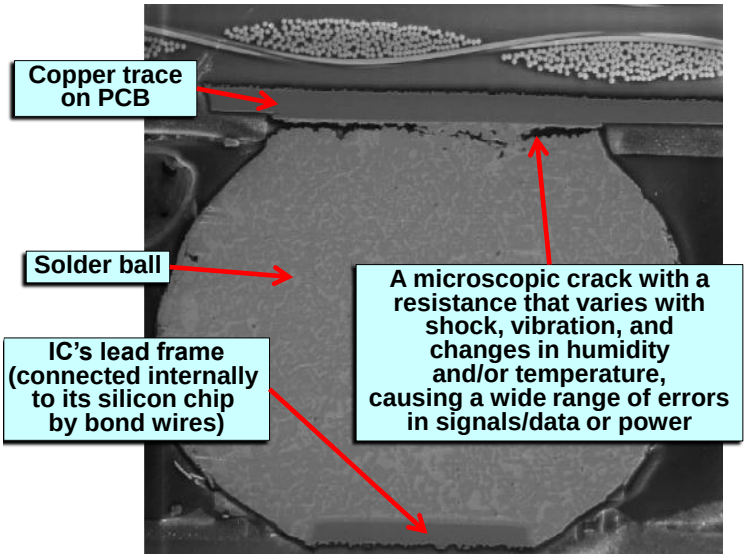
- Demonstrations
- Checklists
- Inspections
- Walk-throughs
- Reviews
- Assessments
- Audits.

Each of these can use one or more of the following analysis techniques:

- Inductive
- Deductive
- "Brainstorming"
- Validated computer modelling
- Testing.

Functional Safety designers and their assessors have become very skilled with using these methods, *but they were never designed to deal with EMI*. To help achieve EM Resilience, they should be competently modified or extended.

A good example is the solder joint as shown below:



Clearly, slight movements due (for example) to changes in temperature and humidity can cause the resistance of this solder joint to vary over a wide range, and vibration can modulate the value of its resistance causing what is sometimes called "mechanically induced EMI."

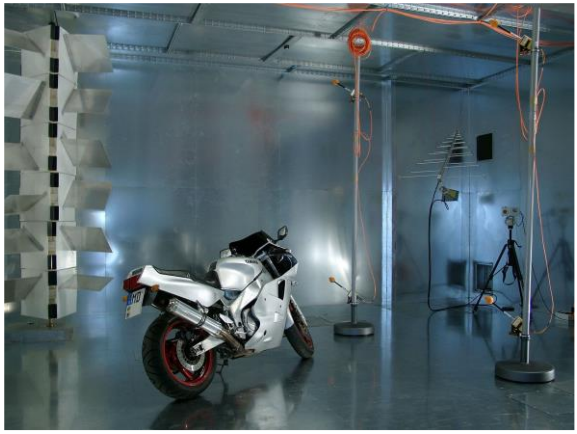
For these reasons, [5] and [6] recommend that all verification and validation techniques be competently modified to take full account of EMI. In particular, they need to take account of the following facts peculiar to EM disturbances:

- EMI can cause one or more signals, data and/or controls to suffer from an almost infinite variety of degraded, distorted, delayed, re-prioritized, intermittent and/or false values
- EMI can cause one or more power supplies to suffer from an almost infinite variety of waveform distortions, overvoltages, undervoltages (dips, dropouts, interruptions, etc.)
- The above EMI effects can all happen simultaneously (i.e. everything can go wrong at once, in any number of different ways), or they can happen in any time sequence that could have critical safety consequences.

A wide variety of test methods has been developed over many decades to help prove that hardware and/or software will be sufficiently reliable, and these should be used wherever appropriate, taking into account both the application and the acceptable level of Functional Safety risk.

Techniques similar to HALT (Highly-Accelerated Life Testing) are also recommended to help prove that the physical implementation will be reliable enough over the entire lifecycle, including mechanical structures, electrical connections, printed circuit boards, solder joints, etc., to help ensure that the SRS will remain compliant with all relevant immunity test standards over its entire lifecycle, as mentioned previously.

There are significant benefits to be had by extending the standardized EMC tests, and by adding non-standardized EMC tests/checks, to help verify and validate that the EM resilience is sufficient. For example, standard immunity tests can be extended by using (see [8], [9]):



- Increased frequency ranges, both lower and higher
- Higher test levels
- More angles/polarizations in radiated testing, e.g., by using reverberation chamber testing as shown in the figure opposite
- Frequencies that a design is especially susceptible to, stimulated by the carrier frequencies themselves, or by demodulation or intermodulation [10]

During any immunity testing, all variations in functional performance should be recorded and analysed afterwards to see if they could have any possible relevance for the Functional Safety risks of the final SRS. This is especially important when EMC laboratory testing is only performed on individual sub-systems, and not on the final SRS as installed.

For example, a fast transient burst might cause a DC power converter to shut down for a second or two to protect itself from damage, which might be perfectly acceptable *in the context of the power converter unit itself, alone*. But when it is powering a microprocessor that must continue to operate correctly to ensure Functional Safety, the time the processor takes to reboot after such a power interruption might not maintain acceptable safety risk levels. This simple example shows that what is acceptable for an individual element of an SRS, might be completely unacceptable for that SRS as a whole. Careful and competent post-testing analysis is therefore necessary.

A useful verification and validation T&M for EM resilience is to repeat the standard or extended immunity tests on units during and after accelerated aging to simulate the effects of the foreseeable physical, climatic and user environments over the lifecycle.

Many manufacturers build two prototypes, one of which goes for HALT testing and one for EMC testing. But they generally don't take a HALT tested (but operational) unit and quickly

recheck its immunity, to see if its EM mitigation needs to be more robust, or if a planned maintenance schedule is necessary to ensure that EMC compliance is maintained throughout the lifecycle.

More information on T&Ms for EMI resilience is given in [11], and [5] [6] provide more detail.

Conclusions

EMC immunity testing alone cannot ensure acceptable Functional Safety risks, however high the test levels used [1] [2]. The only practical techniques that we know of at the time of writing, which can be used to demonstrate that EM disturbances will not cause Functional Safety risks to exceed acceptable levels are:

- The ruggedized high-specification well-maintained EM mitigation 'military' approach
- The "EM Resilience" approach, which applies a suitable combination of techniques and measures as described in the IET's 2017 guide [5] and the forthcoming IEEE Standard 1848 [6]. Other T&Ms that provide the same resilience for all foreseeable EM disturbances may be used instead.

EM Resilience is too new to be able to describe case studies, but because its methodology is based on small and rather obvious extensions to what Functional Safety and EMC engineers have been doing very successfully for more than two decades, no great difficulties are anticipated.

References

[1] K. Armstrong, "Why EMC Immunity Testing is Inadequate for Functional Safety", IEEE 2004 Int. EMC Symp. Santa Clara, CA, August 9-13, ISBN: 0-7803-8444-X

[2] K. Armstrong, "Why increasing immunity test levels is not sufficient for high-reliability and critical equipment", IEEE 2009 Int. Symp. EMC, Austin, TX, August 17-21, ISBN: 978-1-4244-4285-0

[3] K. Armstrong, "Why Do We Need an IEEE EMC Standard on Managing Risks?" 2016 IEEE EMC Magazine – Volume 5 – Quarter 1, ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7477140

[4] "Overview of techniques and measures related to EMC for Functional Safety", The IET, 2013, www.theiet.org/factfiles/emc/emc-overview.cfm

[5] "Code of Practice on Electromagnetic Resilience", The IET, 2017, www.theiet.org/resources/standards/emr-cop.cfm

[6] IEEE Standards Association, project P1848, "Techniques and Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetic Disturbances", standards.ieee.org/

[7] Yuvin Chinniah, "Analysis and prevention of serious and fatal accidents related to moving parts of machinery", Safety Science 75 (2015) 163-173, www.elsevier.com/locate/ssci

[8] K. Armstrong, "Testing for immunity to simultaneous disturbances and similar issues for risk managing EMC", IEEE 2012 Int. Symp. EMC, Pittsburgh, PA, August 5-10, ISBN: 978-1-4673-2059-7

[9] W. Radasky and K. Armstrong, "Non-Standardized Immunity Test Techniques to Help Manage Risks caused by EM Disturbances", IEEE 2016 Int. EMC Symp., Ottawa, Canada, July 2016, ISBN: 978-1-5090-1441-5 (USB) or 978-1-5090-1439-2 (CD-ROM)

[10] Dipl. Ing. (FH) W. Grommes and K. Armstrong, "Developing Immunity Testing to Cover Intermodulation", IEEE 2011 Int. EMC Symp., Long Beach, CA, August 15-19, ISBN: 978-1-45770810-7

[11] J. Silberberg and K. Armstrong, "EMC Risk Management", half-day workshop, IEEE 2015 Symp. EMC&SI, Santa Clara, CA, March 15-21, ISBN: 978-1-4799-1991

Copyright of this article remains with the authors.