Another EMC resource
from EMC Standards

Managing Risks Due to EMI Needs More Than Immunity Testing

Helping you solve your EMC problems

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

JULY 2015

IN COMPLIANCE™

THE COMPLIANCE INFORMATION RESOURCE FOR ELECTRICAL ENGINEERS

It's EMC, But Not As We Know It

Managing Risks Due to EMI Needs More Than Immunity Testing

PLUS

Achieving Perfect ESD Audits for S20.20 ESD Control Programs

10 Questions to Ask When Buying a Used Test Chamber

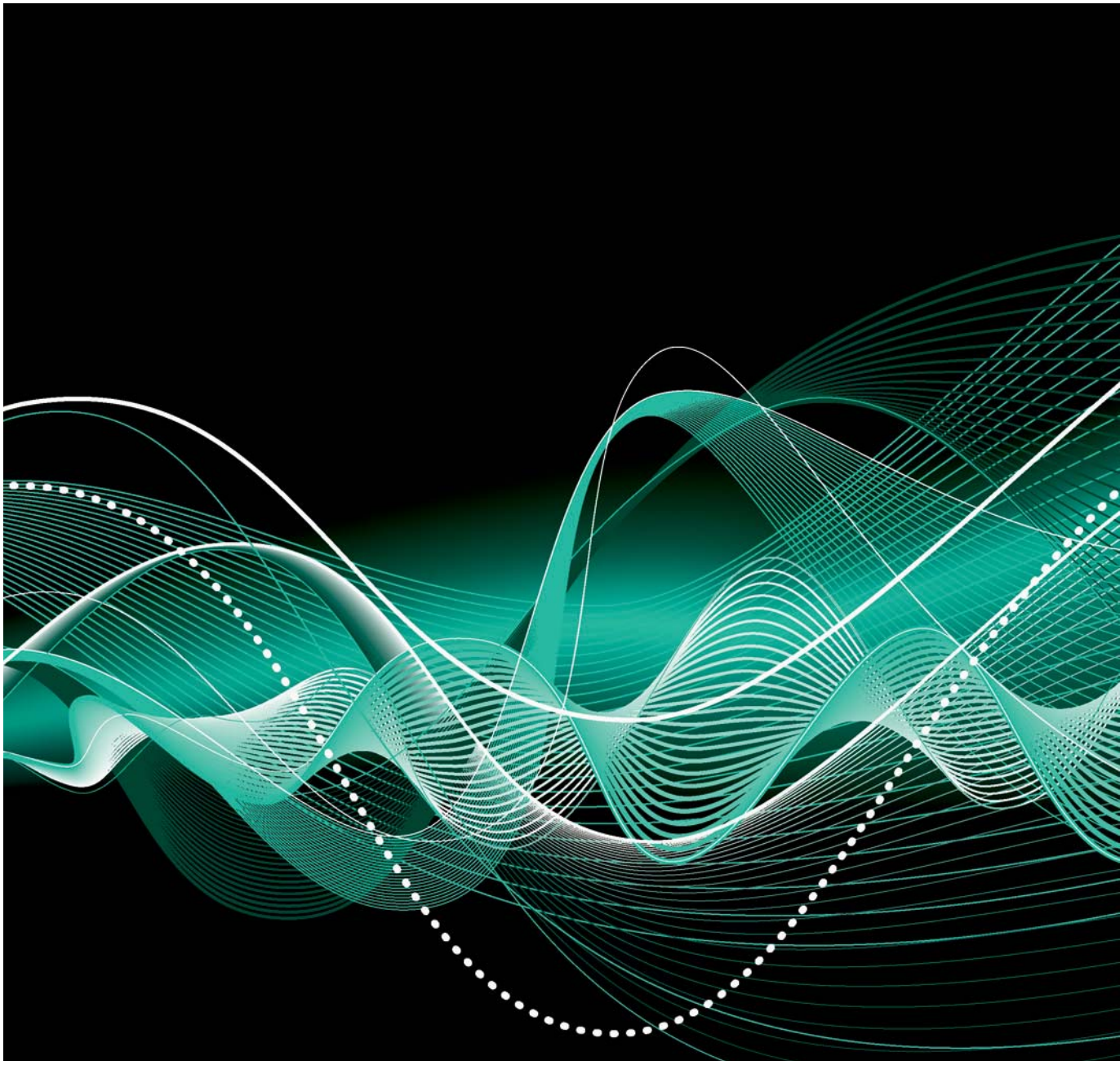
Some Thoughts About Interlocks

Understanding Symbols: Laser Labeling

IT'S EMC, JIM, BUT NOT AS WE KNOW IT!

(with apologies to THE FIRM[1])

Managing Risks Due to EMI Needs More Than Immunity Testing



Keith Armstrong is the founder and principal of Cherry Clough Consultants Ltd, UK based but with clients worldwide, and uses well-proven EMC engineering principles and practices to help companies achieve compliance for their products whilst reducing their costs, timescales and financial risks. Keith can be reached at keith.armstrong@cherryclough.com.

By Keith Armstrong

Welcome to the world of Risk Managing EMC/EMI – where EMC experts meet Functional Safety/Risk experts *and neither side understands anything the other side says*! In this article I hope to be able to explain the risk management of EMI to both EMC experts and Functional Safety/Risk experts, at least so that each engineering discipline is able to begin to communicate with the other.

FUNCTIONAL SAFETY RISKS ASSOCIATED WITH THE INCORRECT FUNCTIONING OF ELECTRONICS

Functional Safety is an increasingly important safety engineering issue that is very different from traditional product safety concerns such as electric shock, fire, heat, etc.

Most traditional safety experts don't understand Functional Safety, and most of the safety standards we traditionally use to show compliance don't address it. So, although being needed for compliance with product liability laws and EU safety directives (e.g., the Low Voltage Directive), it is often completely overlooked, leaving customers exposed to uncontrolled safety risks and manufacturers exposed to uncontrolled financial risks.

Functional Safety compliance should be an important concern for many readers of *In Compliance Magazine*, so I must spend some time describing it. However, it is a large topic so I only have room for an overview.

Almost every aspect of our lives now relies on the correct functioning of electronics, usually programmable electronics (i.e., microprocessors running software programs). In the near future we as individuals and society as a whole will come to rely almost totally on electronics for everything.

Most electronics these days are digital systems, but for at least the last 20 years it has been impossible to fully test even a modestly powerful microprocessor, or a software program larger than a printer driver [2] [3], because:

- Their complexity creates so many possible states that their system could get into that they can't all be tested in any reasonable timescale [2] [3] [4]; and
- Digital systems are discontinuous, non-linear, so testing any percentage of the states that a system could be in cannot predict anything about the untested states [5] [6].

The result of the above two points is that all digital systems can malfunction as the direct result of untested combinations of perfectly correct inputs (i.e., inputs that lie within their specified ranges). In cases in which an electronic system is used in applications where its incorrect functioning could increase safety risks, we say that it presents Functional Safety risks.

Safety and product liability laws and regulations in the developed world generally require an item of equipment not to expose an ordinary user or a third-party to a risk of death at a rate of greater than one in a million per year. This limit applies over the entire lifetime of the equipment, which could in some cases exceed 30 years.

Higher risks than this are generally permitted in cases where a manufacturer shows that the cost of further reducing the risk would significantly outweigh the value of the lives thereby saved, up to a maximum acceptable risk of one death for every 10,000 'informed' users and third parties (i.e., those who have been informed about the risk and have chosen to accept it), and one death for every 1000 'informed' workers, per year.

These safety risk numbers come from a wide range of guidance documents issued by the UK's Health and Safety Executive (HSE) [7]. The legal systems in some other parts of the developed world do not seem to encourage the publication of acceptable levels of safety risks, but everyone surely knows that nothing can ever be perfectly safe.

The problems of not being able to thoroughly test digital systems was first recognized in the 1970s. So, by the 1980s, a huge international effort was underway to try to establish suitable Functional Safety engineering techniques – in system, hardware and software design, and in its verification and validation – to ensure that safety risks could be demonstrated to be acceptably low despite the intractable problems with testing multiple system states.

The first international standard on Functional Safety, IEC 61508 [8], was published in 2000, and a family of application-related Functional Safety standards have been developed from it, including:

- IEC 61511, Safety Instrumented Systems for Process Industry (in USA: ANSI/ISA S84)
- IEC 62061, Safety of Machinery
- IEC 62278 / EN 50126, Railways – Specification and Demonstration of Reliability, Availability, Maintainability and Safety
- IEC/EN 50128, Software, Railway Control and Protection
- IEC/EN 50129, Railway Signalling
- IEC 61513, Nuclear Power Plant Control Systems
- RTCA DO-178B, North American Avionics Software
- RTCA DO-254, North American Avionics Hardware
- EUROCAE ED-12B, European Flight Safety Systems
- ISO 26262, Automobile Functional Safety
- IEC 62304, Medical Device Software

The problems of not being able to thoroughly test digital systems was first recognized in the 1970s. So, by the 1980s, a huge international effort was underway to try to establish suitable Functional Safety engineering techniques.

- IEC/EN 50402, Fixed Gas Detection Systems
- IEC 62304, Medical Device Software
- DEF STAN 00-56, Accident Consequence (UK military)

In cases where a thorough risk analysis shows that imperfect functioning of a digital system could cause unacceptable Functional Safety risks and there are no relevant product-family standards, IEC 61508 should itself be directly applied.

IEC 61508 and its family of Functional Safety standards deal with the impossibility of testing a sufficient proportion of a digital system's states, by:

i) Determining the level of risk that is acceptable, and using this as the basis for…

ii) the appropriate application of a range of well-proven techniques and measures (T&Ms) in…

iii) the design, verification and validation of…

iv) the systems, and the hardware and software that comprise them…

v) all justified in detail in a 'Safety Case'…

vi) with independent assessment of all of the above items…

vii) and, finally, any iteration necessary in the above, to satisfy the assessor.

Even so, complexity still causes difficulties. So, in cases where a control system is very complex, it is normal to identify the functions that are only concerned with managing the Functional Safety risks, and then to remove them into a separate safety-related system (SRS). This is less complex and thus more amenable to using the above process to reduce safety risks to acceptable levels.

In complex systems such as industrial control systems, it is important to understand that the discipline of Functional Safety applies to the entire facility, including the management of its personnel (see Figure 1). The acceptable safety risk level is achieved by the combination of several risk-reduction methods, so the electronic systems do not have to shoulder the whole burden of managing the risk. However, IEC 61508 only provides requirements for the SRS's electronic systems.

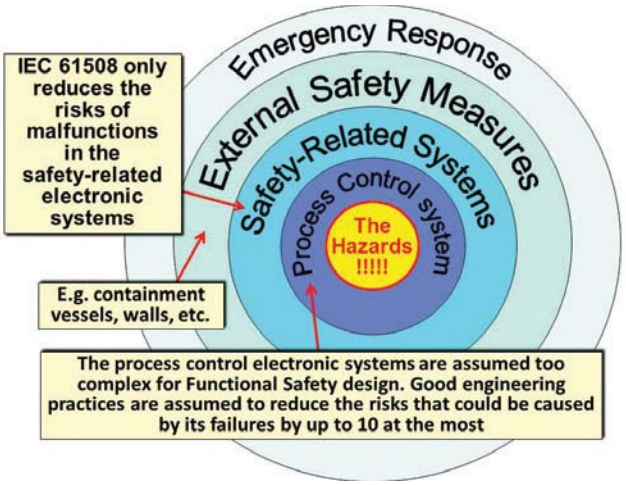


Figure 1: Example of the Functional Safety of an industrial processing plant

A powerful technique in Functional Safety is to determine one or more "safe states" that the equipment can be switched into by the SRS when it detects the potential for a hazard. For example, opening a machine guard causes the machine's SRS to stop the machine quickly enough to avoid injury.

Clearly, there are other applications in which all of the Functional Safety requirements may have to be provided solely by electronic systems, for example, for a patient in a medical ventilator, a space-walking astronaut's space suit, a deep-sea diver's rebreathing system, a heart pacemaker, etc. Some of these examples count as life-support, and so may have no safe states to be switched into. They must keep operating at least well-enough to prevent death or injury, and IEC 61508 also includes T&Ms suitable for this type of application.

MEDICAL RISKS ASSOCIATED WITH THE INCORRECT FUNCTIONING OF ELECTRONICS

Medical devices are subject to the requirements of a basic functional safety standard other than IEC 61508. That standard, ISO 14971, uses completely different terminology and, unfortunately, does not provide a practical process for compliance similar to that found in IEC 61508 (the i – vii list above), resulting in all manner of practical difficulties for managing medical risks that could be caused by the incorrect functioning of electronics. (Further discussion on this point is beyond the scope of this article, but read [9] if you are interested.)

OTHER RISKS ASSOCIATED WITH THE INCORRECT FUNCTIONING OF ELECTRONICS

There are many other kinds of non-safety risks that can be caused by electronic systems that don't function correctly, including (for example): economic; financial; timescale; contractual; etc.

Whatever the kind of non-safety risk, once an acceptable risk level has been agreed for an application, the process by which the relevant electronics is designed, verified, validated and assessed can then follow the IEC 61508 methodology.

MANAGING FUNCTIONAL SAFETY (AND OTHER) RISKS DUE TO EMI

All electronics can suffer from errors, malfunctions and/or failures due to electromagnetic interference (EMI), so EMI must be taken into account when complying with Functional Safety. When applying IEC 61508 or its family of Functional Safety standards, it is typical to allocate one-tenth of the acceptable risk level to EMI unless there are special circumstances. So, for example, if a digital system must maintain a risk of less than one death per million per year over its complete lifecycle, then the risk of EMI causing it to suffer an error, malfunction or failure that could lead to a death must be less than one in 10 million per year.

Electromagnetic compatibility (EMC) is traditionally assured by laboratory testing. Where safety risks are concerned, it is usual to apply the standardized immunity tests at higher levels while ensuring that the equipment continues to operate correctly. This method has been recognized as being inadequate, on its own, for Functional Safety compliance since 2004 [10]. Yet, it is still often relied upon, exposing people to uncontrolled safety risks and manufacturers to uncontrolled financial risks.

Figure 2: Some 'Big Grey Box' examples

Immunity testing on its own is inadequate because, as previously discussed, it is physically impossible to test all the possible states of a digital system thoroughly enough to prove compliance with Functional Safety. Remember, unlike an analogue system, it is impossible to predict what an untested state of a digital system will actually do [2] [3] [5] [6].

Further, safety risks must be low enough over the whole lifecycle of an SRS. So trying to prove compliance with Functional Safety by EMC immunity testing alone must also take into account the effects on the equipment's EM characteristics of the following reasonably foreseeable issues:

- Corrosion, aging, wear, contamination, etc.
- Faults (e.g., a broken filter ground wire)
- Foreseeable use/misuse (e.g., leaving a shielding door open, replacing a shielded cable with a less-well-shielded type)
- Mechanical stresses and strains that alter the impedances of electrical bonds, EMC gaskets, etc., degrading the performance of shielding and filtering
- The possible range of variations in: transient/surge levels, waveshapes and repetition rates; variations in RF level plus its modulation type, frequency, depth and burst rate, etc.
- Different types of EMI occurring simultaneously or in some critical time sequence, (e.g., RF fields plus ESD, AC power distortion plus a dropout, etc.)
- Reasonably foreseeable combinations of all of the above independent variables.

Even considering just the items in this non-exhaustive list, we very quickly find that attempting to prove Functional Safety compliance over the lifecycle by EMC testing would result in an EMC test plan that explodes to an impractically large size, cost and duration [11].

The traditional way of achieving Functional Safety despite any EM disturbances that could foreseeably arise over a lifecycle is to use rugged, "high-spec" EM mitigation (i.e., shielding, filtering, surge protection, galvanic isolation, etc.). As long as it is sufficiently "rugged," it will maintain high levels of EM mitigation over its entire lifecycle, despite all that could possibly be foreseen, and so it requires deliberate over-engineering.

The military have long employed this approach, which I call the "Big Grey Box" (BGB) method. Some examples are shown in Figure 2.

The problem with the BGB method is that it is too large, heavy or costly for many modern SRSs, especially in avionics, automobiles, portable or implantable medical devices, etc. For this reason, the IEE/IET's Working Group on EMC for Functional Safety developed a practical alternative to the BGB method. This was first published in August 2013 [12] after considerable input from a large number of Functional Safety and EMC experts in the UK.

Whereas the BGB method protects the hardware and software from suffering any significant EMI from the external environment, the IET's 2013 guidance achieves "EMI resilience," which means that the hardware and software could be exposed to significant EMI without affecting its Functional Safety compliance.

Figure 3 shows the basics of this EMI resilience approach, which builds on the existing expertise in the EMC testing and Functional Safety communities.

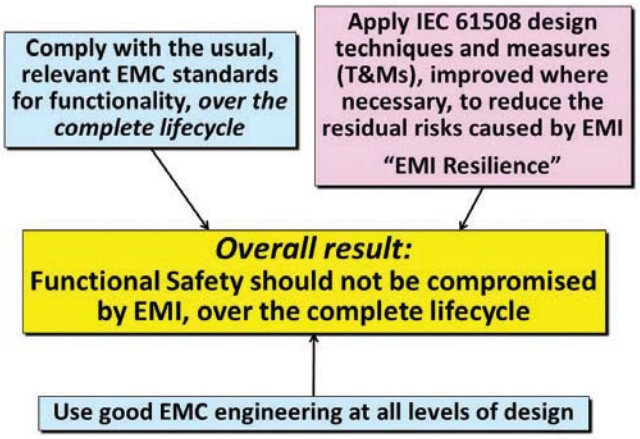


Figure 3: Overview of the IET's 2013 guidance on EMC for Functional Safety

IEC 61508 describes many T&Ms for use in design, to reduce risks caused by errors, malfunctions, faults, etc. in hardware and software to the degree required to comply with Functional Safety. Today, functional safety designers and assessors have become very experienced in their use. These T&Ms operate on the data and other signals (analog, digital, etc.) and/or on the electrical power supplies (AC, DC, etc.), but were never intended to deal with EMI. However, EMI can only affect data, signals and/or power supplies. So it turns out that many of IEC 61508's design T&Ms are very effective in dealing with the effects of EMI.

Accordingly, the IET's 2013 guidance [12] details which of IEC 61508's existing T&Ms are good for dealing with EMI, as well as how to improve their benefits for EMI resilience, while adding a couple of new T&Ms for good measure. None of this requires functional safety designers or independent assessors to know a great deal more than they do at present.

The title of this article is "Its EMC, Jim, but not as we know it" and now we can see why. We are protecting our systems against EMI not by designing shielding, filtering, surge suppression etc. then proving they work by EMC testing, but instead by using clever hardware and software design.

EXAMPLES OF T&MS FOR EMI RESILIENCE

I haven't yet described the IEC 61508-type design T&Ms, so this is a good point to do so. Most designers find that they have at least a passing familiarity with most of them, and they have been used for decades.

Examples of T&Ms for Redundancy and Diversity

- Multiple sensors sense the same parameters
- Multiple copies of data are stored
- Multiple communications carry the same data
- Multiple processors process the same data
- Comparing one with another out of any multiple can detect the presence of errors
- Voting, for example any two that agree out of three, can correct errors

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, one of the channels could be inverted, thereby making EMI more likely to be detected by monitoring the difference between their outputs, at no extra cost.

Examples of T&Ms for Error Detection & Correction Codes

- Error detection coding (EDC) means adding redundant data to make errors detectable.
- Error correction coding (ECC) means adding enough redundant data that corruption is not only detected but the data can be restored to the desired level of accuracy.

Both of the above have been widely used for decades. In fact, it would not be possible for us to have CDs, DVDs, or the Internet without them.

Examples of T&Ms for Static and Dynamic Self-Testing

- Static self-testing checks the hardware and software before operation begins, and prevents start-up if necessary.
- Dynamic self-testing checks that the operation of the hardware and software is correct during operation, for example by inputting fixed signals/data and checking that the outputs are within the expected boundaries. Critical aspects of data processing might even be checked for correct operation once every second, perhaps even more often.

Examples of T&Ms for Power Supplies

- Window comparators check that external power supplies are within design limits.
- Stored energy (e.g., batteries, supercapacitors) is 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) are operated in parallel (e.g., so-called N+1 redundancy) so that the failure of one or more power sources 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 sufficient EMI Resilience

- Some EMI resilience T&Ms will probably have already been chosen for other Functional Safety reasons, and some of them may be able to be modified to improve their benefits for EMI resilience.
- Additional EMI resilience T&Ms may need to be employed to achieve sufficient EMI resilience overall.
- In a system, some items of equipment may rely on EMI resilience T&Ms, while others use the BGB approach.

THE NEED FOR EMC TESTING

It is possible to rely solely on IEC 61508 design T&Ms to create functionally safe systems, but they can suffer too much downtime (i.e., have unacceptably low availability) because EMI can make them fail to start up, or switch to their safe states, much too frequently. Such systems can be expected to be modified by their users or owners to improve their availability (usually by disabling the SRS). Under product liability laws in the EU, any subsequent injuries or damage would be the manufacturer's fault, because the user's modifications

to get their equipment to actually operate more of the time are reasonably foreseeable.

Achieving adequate availability simply needs compliance with the normal, relevant EMC immunity standards, which have all been developed over time for specific applications and/or EM environment(s). These include, for example, the immunity test standards that have been used for decades for compliance with the EMC Directive, and customer-specific EMC specifications for railway signalling, automobiles, military equipment, avionics, etc.

The EMC community has extensive experience in conducting such testing, but it is not enough for Functional Safety for equipment merely to pass its EMC tests when shiny and new. The IET's 2013 guide requires equipment with Functional Safety compliance requirements to maintain its ability to pass all of its relevant EMC standards *throughout its entire lifecycle*. I visualize the combination of EMI resilience T&Ms with lifetime-reliable EMC test standard compliance to work as follows:

- The low-cost, lightweight, non-BGB EM mitigation (shielding, filtering, surge suppression, etc.) attenuates all normal EM disturbances sufficiently for the EMI experienced by the hardware and software to be below its noise thresholds;
- If there is an extreme or unexpected EM disturbance, and/or a combination of EM disturbances, and/or if the EM mitigation degrades or fails (it is not as rugged or expensive as BGB), and/or whatever else happens so that EMI exceeds the noise threshold and corrupts signals, data and/or power supplies: the EMI resilience T&Ms kick-in and do whatever is necessary to maintain Functional Safety, for example, by switching to an unaffected back-up system.

T&MS FOR DESIGN VERIFICATION AND VALIDATION

No single verification or validation method is comprehensive enough to prove that a design is functionally safe. So it is necessary for several different verification or validation methods to be applied by designers who verify system, hardware and software designs and by independent assessors who validate those designs. Applicable verification and validation methods include (but are not limited to):

- Demonstrations
- Checklists
- Inspections
- Walk-throughs
- Reviews
- Assessments
- Audits
- Other approaches not listed here

And each of the above can use one or more of the following techniques:

- Inductive design analysis
- Deductive design analysis
- "Brainstorming" design analysis
- Validated computer modelling
- Testing (which is the most costly and time-consuming method for verifying designs)

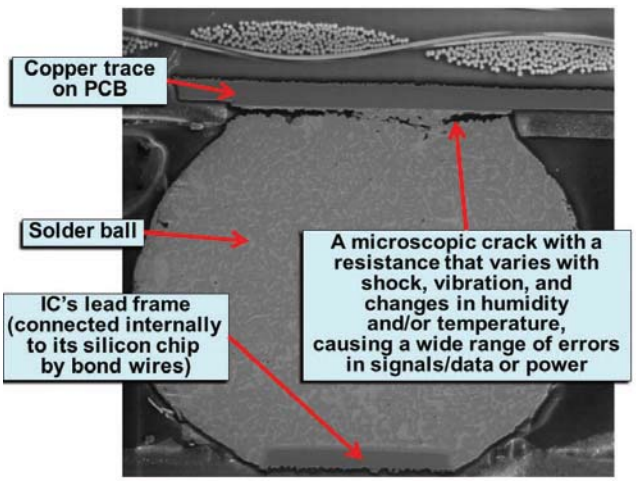


Figure 4: Microscopic cross-section of an intermittently failing IC solder joint (from Michael Pecht *et al*, *Journal of Microelectronics Reliability*, Apr 2008)

The above is the normal method presented in IEC 61508 and its family of Functional Safety standards, which provide detailed guidance on the methods considered appropriate for verifying and validating system, hardware and software design, according to the acceptable level of Functional Safety risk. Since 2000, when IEC 61508 was first published, Functional Safety designers and their independent assessors have become very skilled with using them.

However, these verification and validation T&Ms were never designed to deal with EMI. So, to help achieve EMI resilience, they generally need to be competently modified and/or extended.

In particular, they need to take account of the fact that:

- EMI can cause one or more signals, data and/or controls to suffer from an almost infinite variety of degraded, distorted, delayed, re-prioritised, 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.

For example, many failure mode effects analyses (FMEAs) simply go around every solder joint of every circuit component, determining the possible consequences if it is stuck high or stuck low. But what about the real-life example of the solder joint in Figure 4? Clearly, its resistance can vary over a huge range of values over a period of time, and vibration can even modulate it, giving rise to what is sometimes called "mechanically induced EMI."

TEST METHODS

A wide variety of test methods have been developed to help prove that hardware and/or software can be relied upon, and they should be used where appropriate, taking into account both the application and the acceptable level of Functional Safety risk. Highly-accelerated life tests (HALTs) 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.

Figure 5: Example of a reverberation or stirred-mode chamber: The (large) Reverberation Chamber at Otto-von-Guericke-University Magdeburg, Germany

ADDING EMC CHECKS AND/OR EXTENDING THE STANDARD EMC TESTS

Compliance with the relevant immunity test standards over the entire lifecycle is required, and was discussed above. But the standard EMC tests can be extended, and non-standardized EMC checks can be added, to help verify and validate that the EMI resilience is sufficient. For example, the standard EMC tests can be extended by using:

- Increased frequency ranges (lower and higher)
- Higher test levels [13]
- More angles/polarizations in radiated testing (e.g., by using reverberation chamber testing, see Figure 5)
- Frequencies that a design is especially susceptible to, either stimulated by the carrier frequencies themselves, or by demodulation or intermodulation [14].

The sooner we all start properly managing the effects of EMI on safety and other risks, the better.

During any testing, all variations in functional performance should be recorded, and analyzed afterwards to see if they could have any possible relevance for the Functional Safety risks of the overall safety system.

This is especially important in larger systems where EMC laboratory testing might only be able to be performed on individual sub-systems, and not on the overall system or installation. 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. In the context of the power converter unit itself, this might be considered perfectly acceptable. But when it is powering a microprocessor that must continue to operate correctly for reasons of Functional Safety, the time the processor takes to reboot after such a power interruption might not be safe enough.

Another good verification and validation T&M for EMI resilience is to repeat the standard or extended EMC 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 often miss a useful trick by not taking the HALT tested unit and quickly rechecking its EMC 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.

For more information on T&Ms for EMI resilience, see [15] or [16]. For even more detail, read [12].

SUMMARY AND CONCLUSIONS

Neither the achievement of Functional Safety nor the management of any other kinds of risks that depend upon the correct functioning of digital electronics can be assured by EMC immunity testing alone [11], however high the test levels are set [10]. The only practical techniques that I know of at the time of writing that can be used to prove that EMI will not cause Functional Safety or other risks to increase above acceptable levels are:

- The "Big Grey Box" approach (rugged high-spec EM mitigation)
- The "EMI resilience" approach based on applying a suitable combination of techniques and measures as described in the IET's 2013 guide [12], or other techniques and measures that provided the same resilience for all foreseeable effects of EMI.

My hope is that this article has communicated something useful on EMC/EMI to Functional Safety engineers, and something useful on Functional Safety to EMC/EMI engineers. The sooner we all start properly managing the effects of EMI on safety and other risks, the better.

REFERENCES

1. The Lyrics of Star Trekkin', a record by The Firm, 1987, for example visit http://en.wikipedia.org/wiki/Star_Trekkin%27
2. "*Our programs are often used in unanticipated ways and it is impossible to test even fairly small programs in every way that they could possibly be used. With current practices, large software systems are riddled with defects, and many of these defects cannot be found even by the most extensive testing. Unfortunately, it is true that there is no way to prove that a software system is defect free.*" An extract from: "The Quality Attitude," Watts S. Humphrey (often called "The Father of Software Quality"), Senior Member of Technical Staff, Software Engineering Institute, Carnegie Mellon University, USA, in "News at SEI," March 1, 2004: www.sei.cmu.edu/library/abstracts/news-at-sei/wattsnew20043.cfm
3. "*We no longer have the luxury of carefully testing systems and designs to understand all the potential behaviours and risks before commercial or scientific use.*" An extract from: "A New Accident Model for Engineering Safer Systems," by Professor Nancy Leveson, Professor of Aeronautics and Astronautics, and Professor of Engineering Systems, Massachusetts Institute of Technology

(MIT), USA, in: "Safety Science," Vol. 42, No. 4, April 2004, pp. 237-270: http://sunnyday.mit.edu/accidents/safetyscience-single.pdf

4. "*With autonomous driving new questions arise. To do automated braking you need a certain amount of validation. We have looked at what it takes to validate autonomous driving, and the time needed was estimated at 100,000 years. We need breakthrough solutions from the research community.*" A quote from Michael Bolle, president of Corporate R&D at Robert Bosch, from "Car safety and the digital dashboard" by Chris Edwards, in E&T, the magazine of Institution of Engineering & Technology, vol. 9, iss. 10, 13 October 2014, http://eandt.theiet.org/magazine/2014/10/car-safety.cfm

5. "*Computer systems lack continuous behaviour so that, in general, a successful set of tests provides little or no information about how the system would behave in circumstances that differ, even slightly, from the test conditions.*" An extract from: "Computer Based Safety-Critical Systems," The Institution of Engineering and Technology, UK, Sept. 2008: www.theiet.org/factfiles/it/computer-based-scs.cfm?type=pdf

6. *"If you go to the Museum of Science and Industry in Manchester… …You stand there looking at the rods and the cogs and the flywheels pumping and churning away and you think, "That piston will hit that wheel next time round." But it never does. Everything misses everything else by exactly the same margin every time. For ever. Electrical equipment, however, is different. It can do the same thing over and over and over again, but then one day it will just freeze and you have to turn it off and then on again, or tap the viewing card with your teeth, or unplug the system and leave it be for three minutes."* An extract from: "A brilliant feat of pointless engineering? Guilty as charged," by Jeremy Clarkson, presenter of the Top Gear TV show, in 'Driving', Sunday Times, 12 January 2014, page 10, www.thesundaytimes.co.uk/sto/ingear/clarkson/article1360561.ece

7. For many very useful free HSE publications on Risk Assessment, visit www.hse.gov.uk/pubns and search by "ALARP risk assessment," the most relevant documents will appear on the first and second pages of results and can be downloaded as PDFs.

8. IEC 61508 "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems," in seven parts, available from https://webstore.iec.ch and other providers

9. "Why few (if any) medical devices comply with their EMC standard, and what can be done about it," Keith Armstrong, IEEE 2014 International Symposium on EMC, Raleigh, NC, August 3-8, ISBN: 978-1-4799-5543-5

10. "Why increasing immunity test levels is not sufficient for high-reliability and critical equipment," Keith Armstrong, IEEE 2009 International Symposium on EMC, Austin, TX, August 17-21, ISBN: 978-1-4244-4285-0

11. "Why EMC Immunity Testing is Inadequate for Functional Safety," Keith Armstrong, IEEE 2004 International Symposium on EMC, Santa Clara, CA, August 9-13, ISBN: 0-7803-8444-X

12. "Overview of techniques and measures related to EMC for Functional Safety," published by the IET in Aug 2013, free download from: www.theiet.org/factfiles/emc/emc-overview.cfm

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

14. "Developing Immunity Testing to Cover Intermodulation," Dipl. Ing. (FH) Werner Grommes and Keith Armstrong, IEEE 2011 International Symposium on EMC, Long Beach, CA, August 15-19, ISBN: 978-1-45770810-7

15. "Details of the first practical method for Risk-Managing EMC," a half-day workshop by Jeffrey Silberberg and Keith Armstrong, IEEE 2014 International Symposium on EMC, Raleigh, NC, Aug3-8, ISBN: 978-1-4799-5543-5

16. "EMC Risk Management," a half-day workshop by Jeffrey Silberberg and Keith Armstrong, IEEE 2015 Symp. on EMC, Santa Clara, CA, ISBN: 978-1-4799-1991-8