Another EMC resource
from EMC Standards

IEEE Standards Project P1848: Techniques & Measures to Manage Functional Safety - IWCS 2018

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

IEEE Standards Project P1848: Techniques & Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetic Disturbances

Keith Armstrong[1], Alistair Duffy[2]

[1] Cherry Clough Consultants, Stafford, UK; [2] De Montfort University, Leicester, UK

keith.armstrong@cherryclough.com; apd@dmu.ac.uk

Abstract

The IEEE EMC Society is undertaking the development of this standard to provide a set of practical methods for managing functional safety and other risks due to Electromagnetic (EM) disturbances throughout the life of a product or system.

It would be applied where EM disturbances could cause errors, malfunctions or failures leading to unacceptable risks over the lifetime; whether safety or any other kind of risk is to be managed.

The "autonomization" of society and the constant need for data underlines the criticality of the data infrastructure and the need for the data industry to consider functional safety and other risks associated with electromagnetic disturbances as a significant element of systems design.

This paper overviews the standard and identifies some of the key practices required.

Keywords: Risk, electromagnetic resilience, functional safety.

1. Introduction

This paper discusses the motivation for, and content of, the IEEE EMC Society project 1848 [1] "Standard for Techniques and Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetics Disturbance". The standard is intended to provide guidance on the assessment and application of techniques and measures that can reduce the risks associated with the interfering effects of electromagnetic disturbances on digital electronic systems, especially safety or mission-related systems. The paper "Electromagnetic threats to Ethernet security and resilience" [2] presented at the 2018 IWCS raises issues about electromagnetic resilience that would have been relatively obscure even just a few years ago but yet which are becoming prevalent during the lifetime of the equipment or the families of equipment currently installed. Hence, the need to understand the likely performance of a system in its electromagnetic environment through the lifetime of that system is vitally important, particularly when safety, security or security is involved, but trying to predict the detail of that environment is as challenging as it has been at any time in recent history.

A key aspect of this paper is that Functional Safety (and associated risk management) cannot be tested using conventional electromagnetic, or electromagnetic compatibility testing, yet its design needs to be verified and/or validated in the product or system. The upcoming standard [1] and the related IET Code of Practice [3] define a set of approaches that can assist in achieving this goal.

The paper will address three basic questions:

1. Why isn't traditional electromagnetic compatibility (EMC) testing sufficient?
2. What is the relationship between Electromagnetic Interference and Functional Safety?
3. What approaches are available to assure electromagnetic resilience for Functional Safety.

2. Why isn't traditional EMC testing sufficient?

To answer this question, it is worth first considering Functional Safety. Functional Safety is particularly concerned with errors, malfunctions and faults in the operation of hardware, firmware and software which results in actual or potential safety risks.

It is better defined as *"The part of overall safety that depends on the correct functioning of the Electrical/Electronic/Programmable Electronic (E/E/PE) safety-related systems and other risk reduction measures"*. [4]

It is a sobering thought to realise that most safety failures happen in the design, manufacture and installation phases of the system. A study by the UK's Health and Safety Executive (HSE) for major industrial accidents found that 44% were due to the specification, 15% due to the design or implementation issues in addition to the unintentionally specified-in errors and, on top of this, 6% of the safety failures were as a result of incorrect installation or commissioning [5] .

Clearly, a guarantee of anything being entirely risk free is impossible. A goal should, therefore, be to manage that level of risk, given that a broadly acceptable safety risk can be defined as a risk of death of less than one in a million, per person, per year [6] . A key challenge is that the Functional Safety testing of a digital system is ***impossible***.

A simple view of the numbers involved illustrates the magnitude of the problem. If an EMC test took 1 ms then a simple 8 bit system would have 2^8 possible states, i.e. 256 possible combinations of the logic, taking just over ¼ of a second to perform the tests. If that system is now 32 bits, then the same test would take approximately 50 days running constantly. Should there be 64 bits to deal with then that total test time would rise to about 1/8 the current age of the Earth. If the total number of bits rose to only 69, with 1 ms total test time then the test duration for all states would exceed the current age of the universe!

A differently-formatted version of this paper was presented by Prof. Alistair Duffy at IWCS 2018, www.iwcs.org
The International Cable and Connectivity Symposium, October 14-17, 2018, Rhode Island Convention Center, Providence, Rhode Island, USA

Michael Bolle, Robert Bosch's President of Corporate R&D said:

> *"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.* [7]

Also, John Clegg, Lead: Software Safety Assurance, Air Division, QinetiQ said:

> *"As noted in the Software Systems Engineering Initiative Best Practice* [8]*, for a particular set of inputs, the software will react in the same way each time. The set of inputs is not just the current inputs, but includes all the previous inputs since the software was started. Hence, the failure rate of the software … is hard, if not impossible, to predict, as it depends on knowledge of the residual faults in the software…"* [9]

Clearly, in the context of this paper and that of [1], the inputs for the software needs also to be viewed in light of the operating environment, in this case electromagnetic, because of the potential effects on those inputs. For example, electromagnetic noise could couple to the data or addressing busses causing a 'flipped bit' taking the software to a random address or changing the data to something incorrect (of course, flags or interrupts could be set or suppressed as well). This does not account for other elements that might be more appropriate to an aging system (other than the environment worsening as the pervasiveness of technology increases) such as intermodulation between slightly different frequencies of coupled noise or between coupled noise and an on-board signal, such as a clock.

As a final thought in this section, the previous example gave a numerical indication of how the number of data states can create an unworkable full testing plan. Now consider adding in more realistic electromagnetic testing. For example, what about considering conducted, radiated, electrostatic discharge environments; what about different frequency regimes, different angles of illumination of radiated immunity; what about different configurations of the system under test, with changes in build-specification or different manufacturers' or OEMs' peripherals? This can only result in an impossible test plan becoming … well … even more impossible!

The need to look at managing risks within electronic systems across the anticipated lifetime of those systems without the ability to deterministically test every conceivable state is an important consideration. It is particularly so for safety criticality in infrastructure projects.

The next section looks, in overview, at some of the techniques and measures (T&Ms) for helping in building that confidence.

3. The Need for Techniques and Measures

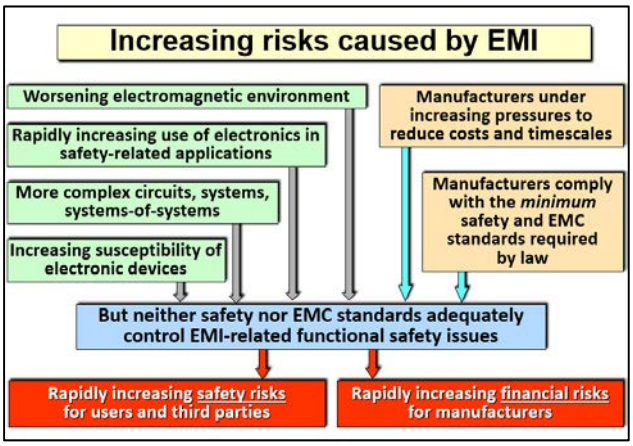
The purpose of [1] is to provide a set of T&Ms to help ensure the specification of the Functional Safety requirements and managing the design, and verifying and validating those designs to ensure that they comply with the original Functional Safety specifications. In particular, the goal is to ensure that all of the possible errors are avoided as far as possible and, if they cannot be avoided, they are detected and corrected to ensure safe operation (perhaps with some degradation to functionality) or the system is switched into one of its safe states.

It is important to recognize that events can happen as one significant major event in any sequence where the order of the events could trigger a hazardous failure or other undesirable event. So, for example, events A, B and C might occur in that or any other order but the order CBA could be the only highly problematic sequence of errors.

It should be noted that functional safety does not take interest in the functionality, even if permanent damage is caused to the equipment, it is simply interested in managing the safety risks and ensuring that they are sufficiently low to meet the needs of the original specifications.

A solution to this requirement is actually to use well proven T&Ms. [4] looks towards delivering a high level of *design confidence* in achieving this Functional Safety by applying an appropriate range of T&Ms and introducing an appropriate level of independent design assessment.

4. The Relationship Between EMI and Functional Safety.



Given the fact that electromagnetic interference, whether natural, man-made ("accidental") or intentional, is a source of compromised performance on all electronic technologies, it cannot be ignored and must be included in any approach to identify and mitigate the Functional Safety risks caused by errors, malfunctions or faults in software systems or the hardware itself.

Figure 1 illustrates the need for EMI to be included in Functional Safety specifications.

Fig. 1 The relationship between EMI and Functional Safety

A differently-formatted version of this paper was presented by Prof. Alistair Duffy at IWCS 2018, www.iwcs.org
The International Cable and Connectivity Symposium, October 14-17, 2018, Rhode Island Convention Center, Providence, Rhode Island, USA

There is, of course, an issue that needs to be bridged. Current Functional Safety practice in industry generally has very little to do with EMC, yet it is clear that compliance with [4] requires managing electromagnetic emissions and the effects of insufficient electromagnetic immunity. This is a clear motivator for [3] and subsequently [1].

It should be remembered that the fundamental expectation is to have a sufficiently high design confidence in the system being considered but no electromagnetic test plan could even come close to being able to provide that, particularly when various tolerances mean that one build is subtly different to the next one, variations and customization in the systems themselves to meet customer needs and expectations; faults; ageing effects; extreme effects in the electromagnetic environment, both acute and chronic. One way to achieve that design confidence would be to over-engineer the product adding extra, and possibly excessive, shielding, filtering surge protection, etc. Not only will this mean that the cost may be prohibitive, the weight and size may also be outside expectations or requirements, which may render the systems unusable for things like automotive or aerospace applications.

Of course, it is important to recognize that any signal, data or control can suffer from a vast array of degradations, distortions, delays, and these can be present on one or multiple signal, data or control lines.

The IET Code of Practice, published in 2017 [3] set out to provide that linkage. The basis was that Electromagnetic Resilience means that Functional Safety integrity should be maintained over all reasonably foreseeable EM disturbances and faults over the lifetime of the System. This relies on:

- Good EM and Functional Safety engineering practices used throughout the design, including appropriate T&Ms.
- Compliance with EMC test standards for emissions and immunity applicable to the normal EM environments expected to be experienced over the lifecycle of the system but assuming that there are no faults *per se*.
- The use of appropriate additional T&Ms to ensure risks remain tolerable, despite reasonably foreseeable EM disturbances *and faults* over the lifecycle of the system.

The IEEE standard [1] uses the IET's Code of Practice as a fundamental building block in its construction.

5. Techniques and Measures

Some common examples of EM Resilience Techniques and Measures include common good design practices such as

- Systems design
    - Physically separating safety and non-safety functions.
    - Partitioning PCBs into different EM zones depending on the nature of the functions being performed by the PCB (such as ensuring that analogue and digital functions are not coincident on the PCB)
    - Specifying practices in the system requirements to include:
        - Redundancy and diversity
        - Error detection and correction
        - Static and dynamic self-testing
- Integration of subsystems, power supplies and communications links.
- Fault monitoring and recording in order to provide diagnostic feedback.

Redundancy is an important elements of EMI resilience, some of the examples that might be considered are:

- Multiple sensors measuring the same parameter
- Storing multiple copies of the same data
- Communicating the same data via multiple channels
- Using multiple processors to process the same data (including e.g. voting to provide the most likely correct approach).
- Using multiple, unsynchronized, clocks
- Using separate power supplies.

The redundancy above can be enhanced if diversity is exploited too. Such diversity may include the use of different physical principles such as different coding schemes for signals and data or using different media types for communications channels. Similarly, it could involve the use of different processor architectures or different algorithms. This diversity may also include designing using independent teams with different experiences and education.

Error detection and correction is widespread in existing technologies such as DVDs, the internet, etc. and is a 'business as usual' component of digital design.

Built in testing and checks are additional techniques and measures for EM resilience:

- Static testing runs diagnostics on the hardware and software prior to commencing operation. Should any anomaly be detected then start-up could be halted.
- Dynamic testing runs diagnostics during operation and allows critical aspects of data processing to be checked for correctness on a near continual basis.

A differently-formatted version of this paper was presented by Prof. Alistair Duffy at IWCS 2018, www.iwcs.org
The International Cable and Connectivity Symposium, October 14-17, 2018, Rhode Island Convention Center, Providence, Rhode Island, USA

Once designs have been generated, it is important to undertake verification and validation. Some common approaches include:

A. Demonstrations
B. Checklists
C. Inspections
D. Walk-throughs
E. Reviews and assessments
F. Audits

These approaches benefit from the application of inductive, deductive and brainstorming design analyses, as well as the development of standardized or bespoke test methods, including highly accelerated life tests. Similarly, the validation of computer modelling is important (and [10] may be useful in providing support for that validation).

An important point above, concerns testing. Standard EMC tests should also be repeated on units as they undergo accelerated ageing of various approaches. Such testing can help test whether electromagnetic compatibility mitigation will degrade or will perform acceptably during the anticipated lifetime of the product. Given that the use of electromagnetic spectrum is extending and increasing, standard EMC tests should be repeated with extended frequency ranges and increased test levels. Similarly, extending the approach to illumination of the test item for immunity tests should also be considered and the use of mode-stirred reverberation chambers might be helpful in performing this sort of investigation. It should also be anticipated that intermodulation susceptibility may increase due to metal junction aging or semiconductor junction ageing and when susceptible frequencies are found, the designer should also consider how this might occur due to multiple source illumination.

Another "extension" of EMC tests is to record all variations in an equipment's functional performance and not just the pass/fail performance that is usually required. The analysis of this data when items of equipment are integrated to create systems helps reveal emergent failure modes, and may also be a topic for future research in the artificial intelligence / big data / grey data domain.

6. Discussion

This paper has discussed the need for techniques and measures to help ensure resilience to electromagnetic disturbances as related to Functional Safety.

It is clear that simply relying on existing EMC tests is insufficient to predict the performance of a system through its lifetime. For one thing, tests are generally retrospective and do not anticipate the environment in which the systems will be operating years into the future.

An overview of a new standard-in-development has been presented, which presents a suite of techniques and measures to ensure design confidence.

Overall improvements in EMC skills and expertise are helpful in developing the tests and interpreting the results in an intelligent and sensible way. However, these cannot be sufficient on their own. The only ways that unacceptable functional safety or other risks can be avoided are by following the T&Ms set out in [1], or by over-specifying and over-engineering the equipment.

References

[1] Armstrong K (WG leader), "IEEE P1848 - IEEE Draft Techniques & Measures to Manage Functional Safety and Other Risks With Regard to Electromagnetic Disturbances/ D5," IEEE, Piscataway, 2018.

[2] A. Duffy, R. Battacharyya and S. Sarma, "Electromagnetic threats to Ethernet security and resilience," in *IWCS*, Providence, RI, USA, 2018.

[3] IET Standards TC4.3, "Code of Practice for Electromagnetic Resilience," IET, London, 2017.

[4] -, "IEC 61508 - Functional Safety of electrical/electronic/programmable electronic safety related systems, ed. 2," IEC, Genever, 2010.

[5] U. H. &. S. Executive, "Out of control. Why control systems go wrong and how to prevent failure" HSG238, 2nd Edition, ISBN 978 0 7176 2192 7, HSE, 2003.

[6] U. H. &. S. Executive, REDUCING RISKS, PROTECTING PEOPLE, HSE's decision-making process", ISBN 0 7176 2151 0, 2001.

[7] C. Edwards, "Car safety and the digital dashboard," *E&T, the magazine of the Institution of Engineering and Technology,* 13 10 2014.

[8] Software Systems Engineering Initiative, "Interim Standard of Best Practice on Software in the Context of DS 00-56 Issue 4," *SSEI-BP-000001,* 1 2009.

[9] J. Clegg, "Challenges for Assuring Software," *Safety-Critical Systems Club (SCSC) Newsletter,* pp. 14 - 18, Jan 2014.

[10] A. Drozd (WG Chair), "IEEE Std 1597.1-2008 - IEEE Standard for Validation of Computational Electromagnetics Computer Modeling and Simulations," IEEE, Piscataway, NJ, USA, 2008.

Biographies

A differently-formatted version of this paper was presented by Prof. Alistair Duffy at IWCS 2018, www.iwcs.org
The International Cable and Connectivity Symposium, October 14-17, 2018, Rhode Island Convention Center, Providence, Rhode Island, USA

Keith Armstrong graduated from Imperial College, London, in 1972 with an Honours Degree in Electrical Engineering.

He has been a member of the IEE/IET since 1977 and a member of the IEEE since 1997. Appointed IET Fellow and IEEE Senior Member in 2010.

After working as an electronic designer, project manager then design department manager, Keith started Cherry Clough Consultants in 1990 to help companies reduce financial risks and project timescales through the use of well-proven electromagnetic engineering design techniques.

Keith has chaired the IET's Working Group on EMC and Functional Safety since 1997 and is the UK's appointed expert to the IEC committees on 61000-1-2 (the basic standard on EMC for Functional Safety), 60601-1-2 (risk management of EMC for medical devices), and 61000-6-7 (generic standard on EMC for Functional Safety).

Since 2015 he has chaired the IEEE Standards P1848 team creating: "*IEEE Standard Practice for Techniques and Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetic Disturbances*".

Alistair P. Duffy received the B.Eng. (Hons.) degree in electrical and electronic engineering and the M. Eng. degree from the University College, Cardiff, U.K., in 1988 and 1989, respectively. He received the Ph.D. degree from Nottingham University, Nottingham, U.K., in 1993 for his work on experimental validation of numerical modeling and the MBA from the Open University in 2003.

He is currently a Professor in electromagnetics at De Montfort University, Leicester, U.K, the Director of the Institute of Engineering Sciences and a Guest Professor at Harbin Institute of Technology, Harbin, China. He is the author of over 200 articles published in journals and presented at international symposia. His research interests include CEM validation, communications cabling, and technology management.

Alistair is a Fellow of the IEEE and of the Institution of Engineering and Technology (IET). He is Vice President for Conferences in the IEEE EMC Society Board of Directors and Associate Editor of the IEEE Transactions on EMC as well as Chair of the IEEE EMC Society Standards Development and Education Committee. He is a member of the Board of Directors of the IWCS.

A differently-formatted version of this paper was presented by Prof. Alistair Duffy at IWCS 2018, www.iwcs.org
The International Cable and Connectivity Symposium, October 14-17, 2018, Rhode Island Convention Center, Providence, Rhode Island, USA