
Another EMC resource
from EMC Standards

# Techniques and Measures to Manage Functional Safety IEEE GEMCCON 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

# Techniques and Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetic Disturbances

Keith Armstrong
Cherry Clough Consultants Ltd, Stafford, United Kingdom
keith.armstrong@cherryclough.com

## 1 Abstract

**Many near-future applications necessary for the safety and quality of human life, will require a huge expansion in high-performance high-power computing; switching power conversion; wireless datacommunications, and wireless power transfer.**

**Electromagnetic interference (EMI) is often ignored at present but will be crucial for the arrival of this future world.**

**Where errors, malfunctions or failures in electronic systems can increase safety or other risks, electromagnetic compatibility (EMC) testing cannot be sufficient for proving that risks are low enough.**

**This paper briefly introduces newly-developed techniques and measures which, when added to traditional EMC testing, can prove that risks due to EMI are adequately low.**

**Keywords—Risk Management; Electromagnetic Compatibility; Electromagnetic Interference; Functional Safety.**

## Table of Contents



## 2 Designing the Future

Autonomous agricultural machines, such as the harvester in Fig. 1, can work 24/7. Some will optimise the growing conditions and pest control for every single individual plant in a field, maximising the yield per acre whilst minimising water consumption.


**Figure 1 An autonomous harvester (Shutterstock_1056325607)**

Autonomous cars will never make human errors, saving hundreds of thousands of lives every year, whilst tripling the maximum traffic-carrying capacity of existing roads. See Fig.2.

Robotic surgeons under the control of human experts, such as the one shown in Fig.3, will perform operations with a finesse no mere human can achieve, improving existing surgery and enabling surgical procedures that are impossible at present.

Top surgical experts will use these robots to perform operations anywhere in the world, without having to travel, increasing their throughput whilst reducing costs per patient.


A differently formatted version of this paper was presented by Keith Armstrong
as the Keynote to the 2018 IEEE 4th GEMCCON, Stellenbosch, South Africa, on November 7, 2018

Figure 2 A Waymo self-driving car (Shutterstock_692545090)

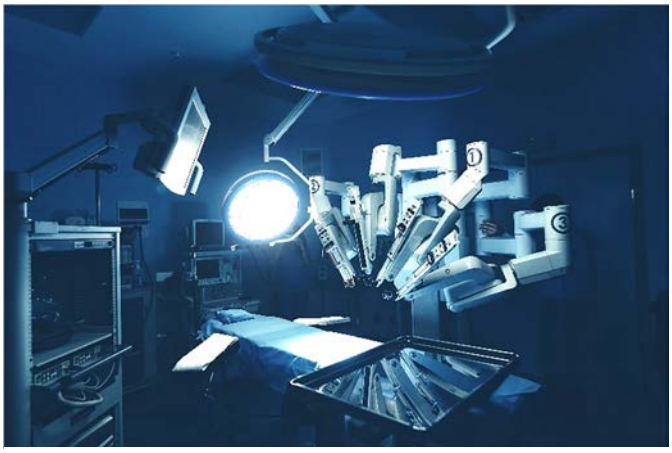

Figure 3 Example of a robotic surgeon (Shutterstock_734373298)

Autonomous mining and extraction machines will operate 24/7 with lower costs and higher productivity than is possible using humans. They will be able to reach deposits in places no human can survive, to extract minerals currently out of reach.

Some companies are developing autonomous mines that automatically load autonomous trains that will take the ore to the docks and automatically load ships.

'Smart' power grids will optimise the use of multiple power sources (fossil fuel, hydro, photo-voltaic, wind, wave, tidal, gases harvested from waste decomposition, etc.) to reduce carbon emissions.

Immersive entertainment will allow everyone to experience individual 'movies', taking the parts of actors.

Figure 4 Example of a Cobot (Shutterstock_1087666304)

Wireless power transfer (WPT) will charge electric cars and buses while they are parked, at up to 7kW across an air-gap. Some companies are working on WPT-at-a-distance, using the same frequencies as Wi-Fi to send watts to equipment anywhere in a room.

Everyone and everything will be uniquely identified and communicable using microwave wireless datalinks: the 'Internet of Everything'.

In industry, 'cobots' (see Fig. 4) will work alongside people without any safety barriers. The author recently saw advertisements for ABB cobots in the public concourse at Changi Airport, Singapore, and BAE Systems expects to have a cobot manufacturing facility operating in the UK by the end of 2018 [1].

Elderly and disabled people will have the support and companionship of personal robots, bathing, dressing, feeding and putting them to bed – according to their individual preferences. Checking their health at least daily and modifying their medications as needed without requiring visits by/to doctors.

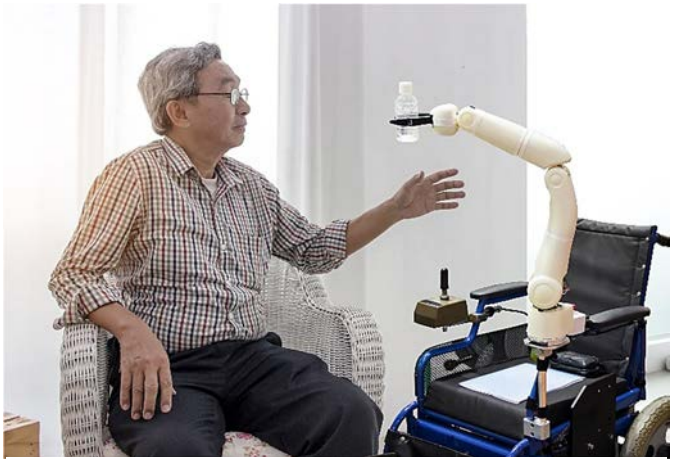

Figure 5 A simple personal care robot (Shutterstock_1099664006)

Fig. 5 shows an example of a simple personal care robot, and many more can be seen in [2].

We know that all of these, and very much more, are achievable and likely to happen, if not now, then in the near future. We need them to increase food production from shrinking agricultural land areas to cope with a doubling in the number of people on the planet.

We need them to help prevent climate change, or cope with its consequences. We need them to be able to continue to provide adequate medical care, and especially to care for elderly people as the earth's population ages. And we need them in order to have something to do with our lives when all the manual and office jobs are replaced by autonomous

robots and artificial intelligences.

Unfortunately, there is a hidden problem that could stop all the above in their tracks. One that is invisible, difficult to understand, unknown to most people and many specialists, and – where known – widely ignored by companies and organisations for whom the next quarter's financial results are the be-all and end-all of their existence.

It is electromagnetic interference, known as EMI.

***Long story, short:***

i) All the above are only made possible by the latest digital processors, which use unimaginably tiny features, sometimes only a few atoms thick.

ii) These processors emit high levels of electromagnetic (EM) noise at high frequencies (up to several GHz at present, higher in the future).

iii) These processors are very vulnerable to errors and malfunctions caused by EM noises in their environments, at frequencies up to many GHz.

iv) Microwave wireless communications will increase EM noise levels considerably, up to many GHz.

v) High-efficiency power converters will emit more EM noise at ever-higher frequencies, at least 1GHz.

vi) Most of these processors will be in close proximity to each other; to wireless radio transmitters, and to power converters.

vii) There will be an exponential increase in the incidence of EMI. From being a fairly rare event, it will become the norm.

viii) It has long been impossible to fully test digital microprocessors or the software that runs on them, and even more impossible to fully test their susceptibility to EMI.

viii) Existing EMC standards cannot ensure freedom from EMI, but EMC standards committees have been unable to cope with the pace of developments in electronics for at least a decade and are slipping further behind.

x) Many standards committees are dominated by organisations who only have short term commercial goals and will not allow the changes needed to keep pace with progress, because they fear they could increase their operating costs.

xi) As far as EMI is concerned, many commercial companies, including some of the largest manufacturers in the world, are behaving as if they were a sports car being constantly accelerated towards a concrete wall, with its driver shouting: "I've been driving this road for years with no evidence of any wall!".

***Long story even shorter:***

For EMI, the past cannot be any kind of guide to the future. And the future is very bleak indeed unless we start dealing with EMI properly.

We now know how to ensure that EMI will not make this future world too unsafe: we must 'risk-manage' the response of electronic systems to the electromagnetic disturbances that can cause EMI. The following sections outline how.

# 3 An Overview of 'Functional Safety'

If incorrect functioning of an electronic system could cause safety risks to increase, these are called 'Functional Safety' risks. In the developed world, safety and product liability laws and regulations generally require such systems not to expose users or third-parties to an 'unacceptable' risk of death, throughout the entire lifecycle of the equipment that is under the control of that system.

The UK's Health and Safety Executive (HSE) has specified the unacceptable level of risk as a risk of death of one in ten thousand per person per year [3]. However, where users and third parties have been informed about the level of risk and have chosen to accept it, the maximum permissible risk of death is increased to one in a thousand per person per year.

For risks at or below these maximum levels, manufacturers must show that they could not have reduced the risks further without spending more than 10 times the value of the lives that would be saved [3]. But where functional safety risks can be shown to be less than a one in a million risk of death/person/year, no further risk-reduction is required.

Functional-safety-related electronics these days are generally digital systems (software programs running on programmable hardware), but for some decades it has been impossible to fully test even modestly powerful microprocessors or software programs, as [4], [5], [6] and the following quotations show:

"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." [7].

"We no longer have the luxury of carefully testing systems and designs to understand all the potential behaviors and risks before commercial or scientific use." [8].

"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." [9]

This is because:

- They have so many possible digital system states that they can't all be tested in any possible timescale; and,
- All digital systems are discontinuous (non-linear), and the behaviour of untested system states cannot be predicted from the behaviour of tested states [9].

This problem was recognized long ago, and huge international effort documented a number of well-proven techniques and measures (T&Ms) for designing, verifying and validating systems, hardware and software. These were incorporated into the first international standard on Functional Safety: IEC 61508 [10], in 2000. This is an IEC Basic Safety Publication [11], and a number of product-family Functional Safety standards has been developed from it, including:

- IEC/EN 50128, Software, Railway Control, Protection
- IEC/EN 50129, Railway Signalling
- IEC 61000-1-2:2016, Achieving functional safety with regard to electromagnetic phenomena
- IEC 61511, Safety Instrumented Systems
- IEC 61513, Nuclear Power Plant Control Systems
- IEC 62061, Safety of Machinery
- IEC 62278 / EN 50126, Railways – Reliability, Availability, Maintainability and Safety
- ISO 26262, Automobile Functional Safety
- EUROCAE ED-12B, European Flight Safety Systems
- RTCA DO-178B, North American Avionics Software
- RTCA DO-254, North American Avionics Hardware

The impossibility of thoroughly testing a programmable electronic system is dealt with by IEC 61508 and its family of standards as follows for each hazard in turn:

i) Determine its acceptable level of risk (from the severity of the hazard and the likelihood of its occurrence).

ii) Determine the actual risk, hence the amount of risk-reduction required to make the risk acceptable.

iii) Use the amount of risk-reduction required as the basis for choosing the most-appropriate application of a range of well-proven T&Ms that address design, verification and validation; for the systems, and for the hardware and software used in their construction.

iv) Justify and describe i) – iii) above in a 'Safety Case'.

v) Have the safety case from iv) assessed, and satisfy the assessor, by iterating the design, verification/validation, etc., where necessary.

The above process has difficulty dealing with great complexity, so it is usual to identify the system functions that are only concerned with managing the functional safety risks of the equipment under control (EUC) and realize them in a separate safety-related system (SRS). The electronic systems in the EUC itself are only required to use good safety engineering practices.

This relatively new safety-engineering discipline of functional safety applies to the entire facility (including personnel management) as indicated by Fig. 6.

IEC 61508 and its 'daughter' standards only have requirements for the SRS. IEC 61508 was written by industrial plant safety experts but can be applied to any functional-safety-related systems. Life-supporting systems might have no safe states to be switched into, and so must keep functioning well-enough to prevent death or serious injury. IEC 61508 also includes suitable T&Ms for this.

Instead of IEC 61508 or any of its family of related standards; medical devices, equipment and systems use ISO 14971 for managing their functional safety risks. It is beyond the scope of this paper to describe the differences [12].

IEC 61508 and its related standards only address functional safety risks, but their general approach can be used to manage any other kinds of non-safety risks that can be caused by malfunctioning electronic systems, for example: mission-critical,

security, economic; financial; timescale; reputational, etc. All that is necessary to be able to apply functional safety's T&Ms, is to be able to quantify their 'hazards' and risks and compare them with what is acceptable to determine the amount of risk-reduction required.

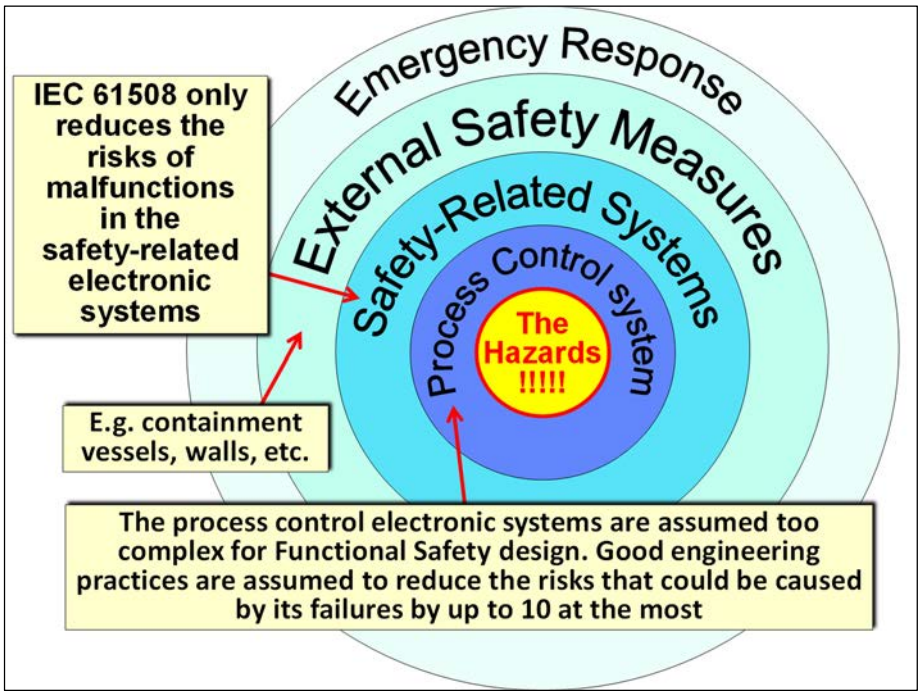


**Figure 6: Illustration of the 'layers' associated with the Functional Safety of an example industrial plant (from [13])**

# 4 The Exploding EMC Test Plan

If we assume that it is possible to test all the states of a programmable electronic system (it isn't), proving that EM disturbances could not cause unacceptable safety risks would require performing immunity tests an impractical number of times to address the following real-life situations:

a) Reasonably foreseeable degradations and failures in EMC-significant components or connections (e.g. connector pins, solder joints, filter ground connections, etc.), throughout the lifecycle. These could be caused by: initial tolerances; aging; corrosion; use/misuse; mis-assembly; temperature/pressure/humidity; vibration; shock, etc.

b) Foreseeable real-life EM disturbances in the system's intended operational environment that varied significantly from the traditional immunity tests (e.g. modulation types/frequencies, transient waveshapes and repetition rates, etc.) to warrant additional immunity tests.

c) Foreseeable combinations of a) plus foreseeable combinations of b), during the lifecycle, for example:
- two or more radiated fields at different frequencies, with a broken 'filter ground' wire;
- a radiated field at any frequency plus an ESD event at any location and any voltage;
- a radiated field at any frequency plus a nearby lightning strike;
- a supply voltage at the low end of its tolerance plus harmonic distortion that reduces its peak height plus a dip, dropout or short interruption, etc.

We very quickly see that trying to cover all these reasonably foreseeable situations over the lifetime would create a "test plan explosion", as Fig. 7 attempts to show. As even one immunity test with one radiated frequency would require an impossibly long time to exercise all of the SRS's digital states, performing all of the complete sets of immunity tests required to fulfil a) – c) above, would be m*ore* impossible.

For more detail on why it is not at all practicable to rely only on EM immunity testing to verify or validate that the risks caused by electromagnetic (EM) disturbances are low enough, see [5], [13], [14], [15] and [16].

# 5 How Can We Risk-Manage EM Disturbances?

The military have traditionally dealt with the above problems by installing their safety-critical systems inside high-specification EM disturbance-mitigating enclosures (using shielding, filtering, surge/transient suppression, fibre-optics, power supply backup, etc.), that are sufficiently rugged not to lose too much of their mitigation's performance between maintenance intervals.

Unfortunately, this method is too large, heavy or costly, or too dependent on maintenance, for many modern SRSs.

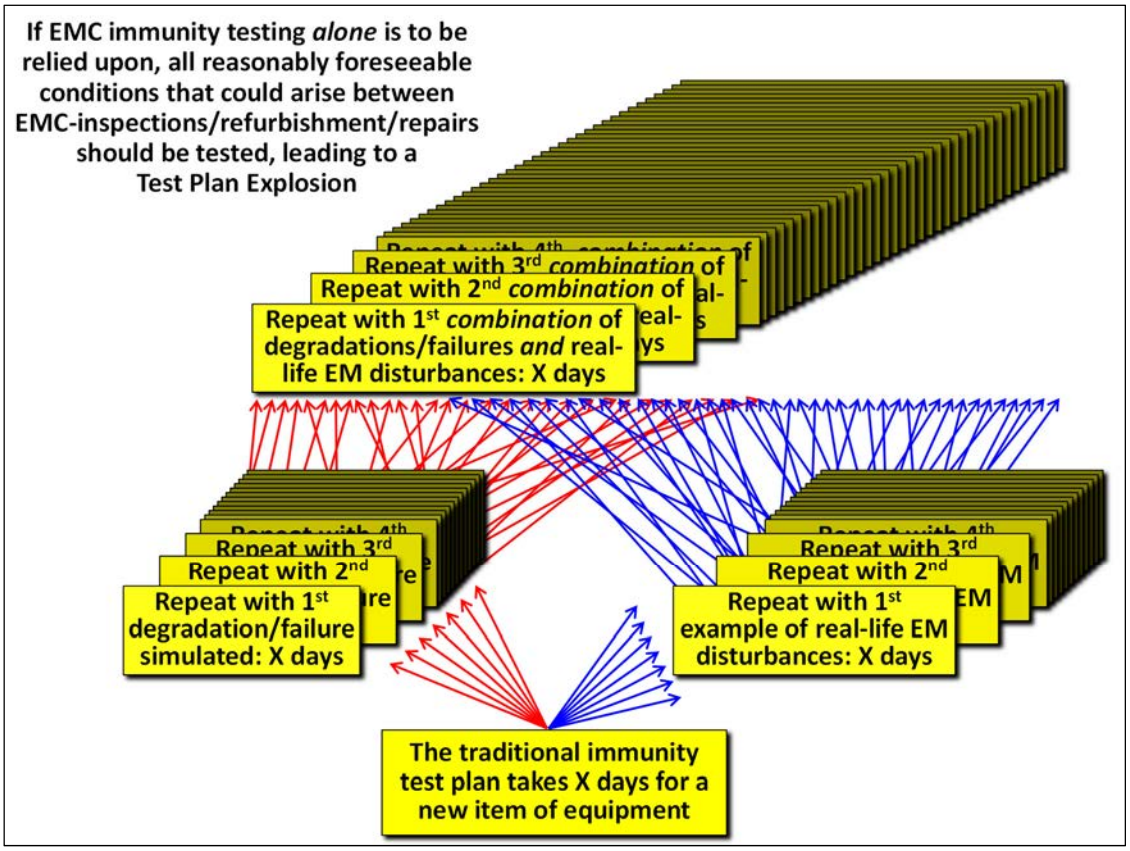


**Figure 7 The problem of the exploding test plan (from [5])**

IEC 61508's design T&Ms try to prevent errors, malfunctions or failures from occurring in signals, data and power supplies, in real-time, during operation. If/when such a problem occurs anyway they detect it, and then either correct it or switch the system into a "safe state", to keep safety risks acceptable.

These design techniques and measures include: error detection / correction coding of data; redundant channels with comparison or voting; redundant power supplies, and a range of other techniques which safety-critical system designers have been familiar with since well before 2000.

Although IEC 61508 says that EMI must be taken into account, it doesn't say how. However, when EMI occurs it actually means that EM disturbances are causing unacceptable errors, malfunctions or failures in signals, data or power supplies, which means that IEC 61508's T&Ms are already quite good at dealing with EMI.

The IET's 2017 Code of Practice [17] and the forthcoming IEEE Standard 1848 [18] identify which of IEC 61508's T&Ms should be used in design and its verification/validation to deal with EMI, and what modifications may be required to some of them to make them truly effective against EM disturbances. They also add some new T&Ms specifically for EMI. For synopses of their practical alternative to the 'rugged high-spec enclosure' approach, see [19], [20].

# 6 Extending Immunity Testing

An SRS must ensure that the risks of the hazards caused by its EUC remain low-enough over its lifecycle [10]. As described in Section III, EM immunity testing cannot be sufficient on its own, however competent EMC test engineers can devise and perform many different types of non-standardized immunity testing, often by extending and/or modifying the standard tests [21], for additional risk-reduction.

These extended tests can help demonstrate sufficient confidence that a given design should not cause unacceptable levels of functional safety or other risks during its lifecycle, as the result of real-life EM disturbances; or as the result of wear, aging, corrosion, and other physical/climatic effects. Examples include extending EM immunity tests to cover:

*i)* *The entire lifecycle*
*ii)* *Simultaneous EM disturbances at a single node*
*iii)* *Simultaneous EM disturbances at two or more nodes*
*iv)* *Modulations to which a design is especially susceptible*
*v)* *Intermodulation*
*vi)* *More angles/polarizations in radiated testing*
*vii)* *Wider frequency ranges*
*viii)* *A wider variety of power quality issues*

# 7 Summary and Conclusions

No amount of EMC testing can prove that the functional safety risks due to the effects of EMI on a programmable electronic system have been adequately reduced.

This paper briefly introduces the newly-developed T&Ms which, added to traditional EMC testing, can demonstrate that risks due to EMI are adequately low.

These T&Ms will be very important indeed for the success of the future world of robotics and autonomous systems.

A tutorial session on the last morning of this Conference will examine the issues raised here in more depth.

# 8 References


[1] Air Force Technology, 29 June 2018, "BAE Systems to pilot cobot manufacturing at Lancashire site", www.airforce-technology.com/news/bae-systems-cobot-manufacturing/

[2] IEEE "Robots", https://robots.ieee.org/

[3] 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 will appear on the first two results pages, and are downloadable as PDFs

[4] "Robustness (computer science)", en.wikipedia.org/wiki/Robustness_(computer_science)

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

[6] J. A. Whittaker, "What Is Software Testing and Why is it so Hard", IEEE Software, Jan-Feb 2000, pp 70-79

[7] Watts S. Humphrey in "The Quality Attitude", March 1, 2004, www.sei.cmu.edu/reports/09sr024.pdf, page 33.

[8] Nancy Leveson in: "A New Accident Model for Engineering Safer Systems", in "Safety Science," Vol. 42, No. 4, April 2004, pp. 237-270, http://sunnyday.mit.edu/accidents/safetyscience-single.pdf

[9] The IET, "Computer Based Safety-Critical Systems" September 2008 (this quote does not appear in the 2013 edition)

[10] IEC 61508 "Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems", in seven parts, available from https://webstore.iec.ch

[11] "Basic Safety Publications", The IEC, www.iec.ch/about/brochures/pdf/tools/BasicSafetyPublications_2011.pdf

[12] K. Armstrong, "Risk Management of Medical Devices Regarding Electromagnetic Disturbances", In Compliance Magazine, January 31st, 2017

[13] How to Manage Risks with Regard to Electromagnetic Disturbances, Keith Armstrong, IEEE 2016 Int. Symp. EMC, Ottawa, Canada, ISBN: 978-1-5090-1441-5 (USB) or 978-1-5090-1439-2 (CD-ROM)

[14] K. Armstrong, "Why EMC Immunity Testing is Inadequate for Functional Safety", 2004 IEEE Int. EMC Symp., Santa Clara, ISBN 0-7803-8443-1

[15] K. Armstrong, "Why Increasing Immunity Test Levels is Not Sufficient for High-Reliability and Critical Equipment", 2009 IEEE Int. EMC Symp., Austin, ISBN: 978-1-4244-4285-0

[16] D. Pissoort and K. Armstrong, "Why is the IEEE developing a standard on managing EMI risks", IEEE 2016 Int. Symp. EMC, Ottawa, Canada, ISBN: 978-1-5090-1441-5 (USB) or 978-1-5090-1439-2 (CD-ROM)

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

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

[19] Prof. D. Pissoort, J. Lanoo, A Degraeve and K. Armstrong, "Risk Management of Electromagnetic Disturbances", Joint IEEE EMC/APEMC 2018, 14-17 May, Singapore, ISBN: 978-1-5090-5996-6

[20] D. Pissoort et al, "Techniques and Measures to Achieve EMI Resilience in Mission- or Safety-Critical Systems", 2017 IEEE EMC Magazine – Volume 6 – Quarter 4

[21] Dr. W. Radasky and K. Armstrong, "Extending the Normal Immunity Tests to Help Prove Functional Safety", Joint IEEE EMC/APEMC 2018, 14-17 May, Singapore, ISBN: 978-1-5090-5996-6