How to Manage Risks with Regard to Electromagnetic Disturbances

Keith Armstrong
Cherry Clough Consultants Ltd
keith.armstrong@cherryclough.com

Abstract

When Functional Safety or other risks must be managed throughout the lifecycle of an electronic system, the acceptable levels for risks that could be caused by electromagnetic (EM) disturbances are so small that they are incapable of being verified or validated by using only immunity testing, even with increased test levels.

After 2000, many safety standards were published that required a risk-based approach to electromagnetic interference (EMI), although until 2013 there were no publications providing any practical guidance on how this could realistically be achieved. The first practical guidance was published in 2013 and is now being incorporated into IEC, IET and IEEE standards, and is the subject of this paper.

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

I. Introduction to Risk Management Safety

Functional Safety is an increasingly important safety engineering risk management issue that is very different from traditional safety concerns such as electric shock, fire, heat, etc., but this paper only has space for a very brief overview.

Where 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 equipment not to expose an ordinary user or a third-party to a risk of death exceeding one in a million per year, throughout the entire lifecycle of that equipment.

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 per year 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 per year for every 1000 'informed' workers. These figures are from guidance documents by the UK's Health and Safety Executive (HSE) [1].

Most electronics these days are digital systems, but for at least the last 30 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 internal system states that they can't all be tested in any possible timescale [2] [3] [4]; and,
- Digital systems are discontinuous, non-linear, so testing any percentage of system states cannot predict anything about the untested states [5].

One result of the above is that all digital systems can malfunction as the direct result of untested combinations of correct inputs (i.e. inputs within their specified ranges) [6].

This testing problem led to a huge international effort starting in the 1980s to try to establish suitable Functional Safety engineering techniques for system, hardware and software design, verification and validation – to make it possible to demonstrate that the functional safety risks of modern digital systems were acceptably low. This effort resulted in the first international standard on Functional Safety, IEC 61508 [7], published in 2000. This is an IEC Basic Safety Publication [8], and a family of application-related Functional Safety standards has been developed based upon 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 – 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

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 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.
ii) Using the level of risk as the basis for the appropriate application of a range of well-proven Techniques and Measures (T&Ms) that address issues of design, verification and validation; for the systems, and for the hardware and software which comprises them.
iii) Describing and justifying all the above in detail in a 'Safety Case', which is independently assessed.
vii) Carrying out any iteration necessary to satisfy the independent Functional Safety Assessor.

Even so, complexity still causes difficulties, so where a

control system is very complex it is normal to identify the functions only concerned with managing the Functional Safety risks associated with the "equipment under control" (EUC), and remove them to a separate safety-related system (SRS). The SRS is less complex and 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 in the SRS do not have to manage the entire risk. Note that IEC 61508 only provides requirements for the SRS's electronic systems.

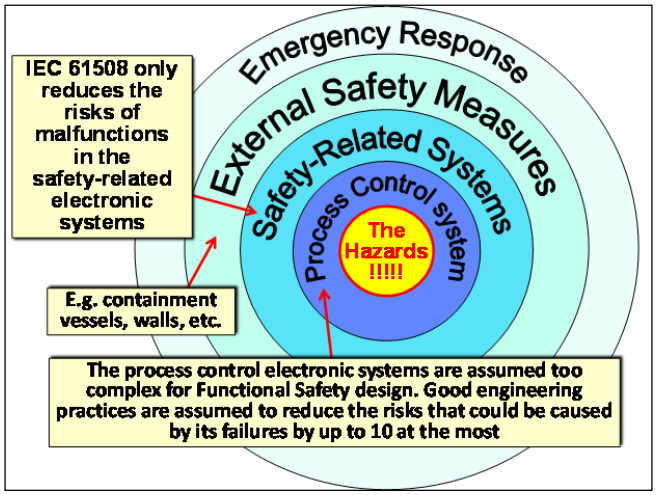

Figure 1: Example of the Functional Safety of an industrial processing plant

A powerful technique in Functional Safety is to determine one or more "safe states" that the SRS could switch the EUC into, if it detects that a hazard is about to arise. For example, opening a machine guard would cause a machine's SRS to stop the machine quickly enough to avoid injury by contact with the now-unguarded hazardous parts.

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 devices are subject to the basic risk management requirements of ISO 14971, not IEC 61508. Further discussion is beyond the scope of this paper, but [9] has more detail.

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; mission; security, etc.

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

II. Introduction to Managing 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 or managing other risks. 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 an SRS is required to maintain a risk of death of 1 ppm (part per million) per person per year throughout its 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 0.1 ppm 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.

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 (and remember, unlike an analog system, it is impossible to predict the behavior of any untested state of a digital system, see [2] [3] and [5]).

Furthermore, the risks to be managed must remain acceptably low throughout the entire lifecycle, so trying to use immunity testing alone must also take into account the lifetime effects on the system's EM characteristics, of *at least* the following reasonably foreseeable issues:

- Corrosion, aging, wear, contamination, etc.
- Faults (e.g., a broken filter ground connection) including intermittent faults, see Figure 2
- 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 modulation type, frequency, depth, 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.

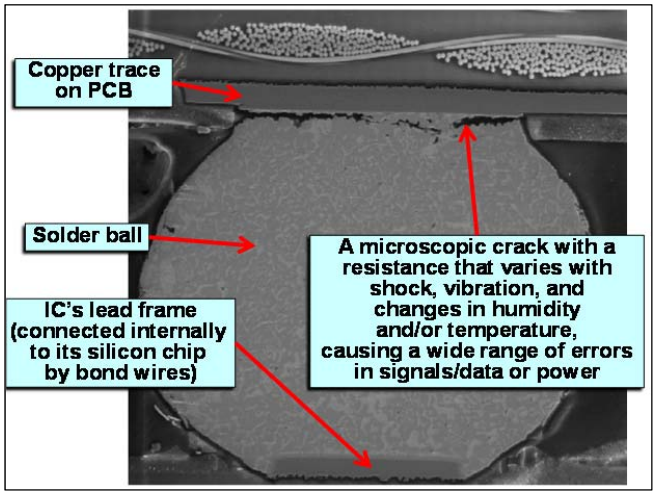

Figure 2: Microscopic cross-section of an intermittently failing IC solder joint (Michael Pecht *et al*, J. Micro. Reliability, Apr 2008)

Even considering the items in the above list, we quickly find that attempting to prove risks will be acceptably low throughout the lifecycle by immunity testing alone, whatever the test levels used [11], causes the EMC test plan to explode to an impractically large size, cost and duration [10] [12].

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 (shielding, filtering, surge protection, galvanic isolation, etc.). It must be sufficiently rugged that it will maintain high levels of EM mitigation between scheduled maintenance/refurbishment activities, despite all that could possibly be foreseen, and so it requires deliberate over-engineering. The military have long employed this approach, which the author calls the "Big Grey Box" (BGB) method. Some examples are shown in Figure 3.

Figure 3: Some 'Big Grey Box' examples

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 IET's Working Group on EMC for Functional Safety developed a practical alternative, first published August 2013 [13] 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 EM disturbances in the external environment, the IET's 2013 guidance aims to achieve "EMI Resilience", meaning that the hardware and software could be exposed to significant EMI without causing unacceptable levels of risk.

Figure 4 shows the basics of this EMI resilience approach, which builds on the existing expertise in the EMC testing and Functional Safety communities.

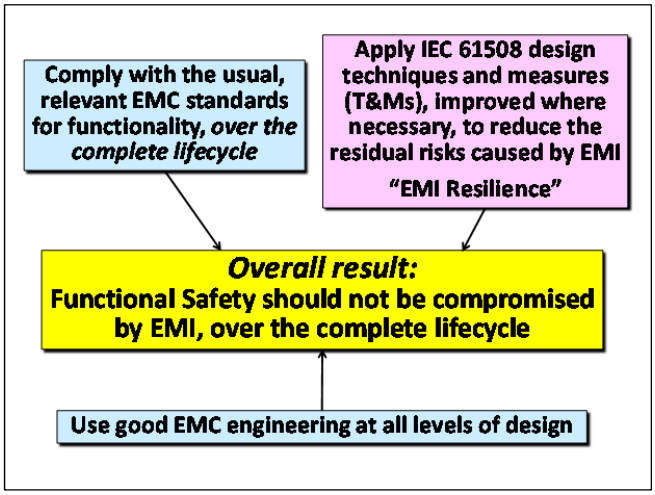

Figure 4: Overview of the IET's 2013 guidance on EMC for Functional Safety

IEC 61508 describes many T&Ms for use in design, verification and validation; for hardware, software and systems; firstly to avoid errors, malfunctions and faults from occurring, and secondly to reduce any remaining risks to conform to the specified risk levels. 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 is commonly found that correct application of IEC 61508's T&Ms is very effective in dealing with the effects of EMI.

Accordingly, the IET's 2013 guidance [13] 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 specifically for dealing with the effects of EMI. None of this requires functional safety designers or independent assessors to know a great deal more than they do at present.

III. EMI Resilience T&Ms in Design

Most electronic hardware, software and system designers find that they are familiar with many of these T&Ms, a high proportion of which 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, 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.

Examples of T&Ms for Error Detection & Correction include:

- Error detection coding (EDC), by adding sufficient redundant data to make errors detectable.
- Error correction coding (ECC), by adding sufficient redundant data that errors are not only detected but the data restored (to a desired level of accuracy).
- 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 inputting fixed signals/data and checking that the outputs are within the expected boundaries. Critical aspects of data processing might be checked for correct operation once every second, perhaps even more often.

Examples of T&Ms for Power Supplies include:

- Window comparators check that 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.

When choosing T&Ms for sufficient EMI Resilience, some appropriate T&Ms will probably have already been chosen for other Functional Safety reasons, and many of them should be able to be modified to improve their benefits for EMI resilience. Additional EMI resilience T&Ms may then 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 rely on BGBs.

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 that keeps switching the EUC into a safe state when it is interfered with, see sections 3.8 and 3.10 in [14].

Under product liability laws (in the EU, at least) it seems that it could be easy to argue that any subsequent injuries or damage were the *manufacturer's* fault, because he should have foreseen that an over-active SRS would likely result in the user modifying their equipment to make it operated as intended most of the time.

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 signaling, 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 [13] requires equipment with Functional Safety compliance requirements to maintain its ability to pass all of its relevant EMC standards throughout its entire lifecycle.

The author visualizes the combination of EMI resilience T&Ms with lifetime-reliable EMC test standard compliance working as follows:

a. 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;
b. 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 as the BGB method), 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 in the SRS kick-in and do whatever is necessary to maintain Functional Safety, for example, by switching the EUC to one of its safe states, or switching in an unaffected back-up control system.

IV. T&Ms in Verification and Validation

No single verification or validation method (such as immunity testing) is comprehensive enough to prove that a design is functionally safe [10] [12]. 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 their independent assessors.

Applicable verification and validation methods include

(but are not limited to): Demonstrations; Checklists; Inspections; Walk-throughs; Reviews; Assessments, and Audits.

And each of the above can use one or more of the following techniques: inductive, deductive and "brainstorming" design analyses; validated computer modelling, and testing.

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 / 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 into account that:

- 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.

For example, many failure mode effects analyses (FMEAs) simply go around each 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 2? Clearly, slight movements due (for example) to changes in temperature and humidity can cause its resistance 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, [13] recommends that all verification and validation techniques be competently modified to take full account of EMI.

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.

Compliance with the relevant immunity test standards over the entire lifecycle is required, and was discussed above. However, there are significant benefits to be had by extending the standard EMC tests and adding non-standardized EMC checks to help verify and validate that the EMI resilience is sufficient. For example, standard EMC tests can be extended (see [15], [16]) by using:

- Increased frequency ranges (lower and higher)
- Higher test levels
- More angles/polarizations in radiated testing (e.g., by using reverberation chamber testing, see Figure 5)
- Frequencies that a design is especially susceptible to, stimulated by the carrier frequencies themselves, or by demodulation or intermodulation (also see [17]).

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 maintain acceptable safety risk levels.

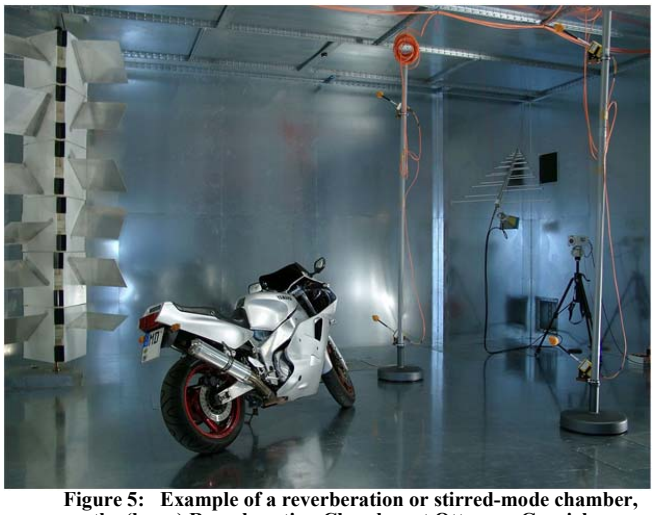

Figure 5: Example of a reverberation or stirred-mode chamber, the (large) Reverberation Chamber at Otto-von-Guericke-University Magdeburg, Germany

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 [18] or [19]. For even more detail, read [13].

V. SUMMARY AND CONCLUSIONS

Neither the achievement of Functional Safety nor the man-

agement of any other kinds of risks that depend upon the correct functioning of digital electronics can be assured by EMC immunity testing alone [10], however high the test levels are set [11]. The only practical techniques that the author knows 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 "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 [13], or other techniques and measures that provided the same resilience for all foreseeable effects of EMI.

Although the EMI Resilience approach has been developed from IEC 61508's Functional Safety T&Ms, they can be used to help manage any kinds of risks that can be caused by errors, malfunctions or failures in modern electronic systems.

EMI 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 insurmountable difficulties are expected.

REFERENCES

[1] 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 and second pages of results and can be downloaded as PDFs.

[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, 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 behaviors and risks before commercial or scientific use."*
An extract from: "A New Accident Model for Engineering Safer Systems", by Nancy Leveson, Professor of Aeronautics and Astronautics, 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 the IET, 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] "Robustness (computer science)", en.wikipedia.org/wiki/Robustness_(computer_science)

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

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

[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, Aug3-8, ISBN: 978-1-4799-5543-5

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

[11] "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

[12] "Why is the IEEE developing a standard on managing EMI risks", Davy Pissoort and Keith Armstrong, IEEE 2016 International Symposium on EMC, Ottawa, Canada, July 2016

[13] "Overview of techniques and measures related to EMC for Functional Safety", published by the IET in Aug 2013, www.theiet.org/factfiles/emc/emc-overview.cfm

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

[15] "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

[16] "Non-Standardized Immunity Test Techniques to Help Manage Risks caused by EM Disturbances", Bill Radasky and Keith Armstrong, IEEE 2016 International Symposium on EMC, Ottawa, Canada, July 2016

[17] "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

[18] "Details of the first practical method for Risk-Managing EMC", half-day workshop, Jeffrey Silberberg and Keith Armstrong, IEEE 2014 Int. EMC Symp., Raleigh, NC, Aug3-8, ISBN: 978-1-4799-5543-5

[19] "EMC Risk Management", half-day workshop, Jeffrey Silberberg and Keith Armstrong, IEEE 2015 Symp. EMC&SI, Santa Clara, CA, March 15-21, ISBN: 978-1-4799-1991-8