Another EMC resource
from EMC Standards

Including EMC in Risk Assessments

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

Including EMC in Risk Assessments

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

***Abstract* – The reliability of electronic technologies (including the software and firmware that runs on them) can become critical, when the consequences of errors, malfunctions or other types of failure include significant financial loss, mission loss, or harm to people, domestic animals or property (i.e. functional safety).**

Electromagnetic interference (EMI) can be a cause of unreliability in all electronic technologies, so electromagnetic compatibility (EMC) must be taken into account when the risks caused by malfunctioning electronics are to be controlled.

However, levels of reliability or safety risk can be three orders of magnitude beyond what could possibly be demonstrated with any practicable EMC testing regime. The challenge for engineers is to demonstrate adequate confidence in the reliability of their designs in the operational electromagnetic environment.

The solution [1] is to use well-proven EMC design techniques, plus risk assessment that shows the overall design achieves acceptable risk levels, all verified and validated by a variety of techniques (including EMC testing).

This paper addresses how to apply risk assessment techniques to issues of electromagnetic compatibility (EMC).

***Keywords* – Cost-effectiveness, EMC, EMI, functional safety, high-reliability, mission-critical, reliability, risk analysis, safety-critical, security, safety risks.**

I. INTRODUCTION

Electronic circuits of all types and the software or firmware that runs on digital processors are susceptible to errors, malfunctions and other types of failure caused by electromagnetic interference (EMI) from the electromagnetic (EM) disturbances they are exposed to over their lifetimes [2].

"High reliability", "mission-critical", "safety-critical" or security applications might need to have a meantime to failure (MTTF) of more than 100,000 years (corresponding to Safety Integrity Level 4 (SIL4) in [3], see Figures 1 and 2).

Some would argue that products that are mass-produced (e.g. automobiles, domestic appliances, etc.) also require very low levels of safety risk, because of the very large numbers of people using them on average at any one time.

EMI has long been recognized as a cause of unreliability in electronic equipment, especially by the military and aerospace industries, and as a result EM immunity test methods and regimes have been developed.

These tests have generally been successful in reducing the failure rate due to EMI. Given the great difficulties in determining whether a given undesirable incident was caused by EMI, the lack of incidents officially assessed as being caused by EMI has led some people to feel that current EMI testing regimes must therefore be sufficient for any application. Indeed, it is commonplace to read words such as "*….passes all contractual and regulatory EMC tests and is therefore totally immune to all EMI.*"

However, as Ron Brewer says in [4]: "*…there is no way by testing to duplicate all the possible combinations of frequencies, amplitudes, modulation waveforms, spatial distributions, and relative timing of the many simultaneous interfering signals that an operating system may encounter. As a result, it's going to fail.*"

Prof. Nancy Leveson says, in [9]: "*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.*"

[10] states: "*Computer systems lack continuous behavior 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.*"

Finally, [11] says: "*Although electronic components must pass a set of EMC tests to (help) ensure safe operations, the evolution of EMC over time is not characterized and cannot be accurately forecast.*"

Any extreme EMC testing regime that has an affordable cost and duration is unlikely to be able to demonstrate confidence in achieving reliable operation at levels above about 90%. The reasons for this are given in [4], [5], [6], section 0.7 of [7], and [8], and show that 90% is a *very* generous estimate.

Since the confidence levels that are needed for functional safety compliance (for example) are a *minimum* of 90% for SIL1 in [3], 99% for SIL2, 99.9% for SIL3 and 99.99% for SIL4, it is clear that more work needs to be done to be able to demonstrate compliance with [3] and similar functional safety standards (e.g. [12] [13] and others such as IEC 61511 and IEC 62061), as regards the effects of EMI on risks.

The best solution at the time of writing is to use well-proven EMC design techniques to reduce risks, and to verify and validate them using a number of different methods, including immunity testing. Risk assessment is a vital part of such an approach, as required by [3]. Unfortunately, neither the IEC's basic publication on Functional Safety [3], nor the basic IEC publication on "EMC for Functional Safety" [1] describes how to take EMI into account during risk assessment; although [7] – a practical guide based on [1] – *does* cover this.

Previous papers by the author covered assessing lifetime electromagnetic, physical and climatic environments [14], appropriate EMC design techniques [15], and verification and validation methods (including testing) [16].

Presented at the IEEE 2010 International Symposium on EMC, July 25-30, 2010, Fort Lauderdale, Florida, USA, ISBN: 978-1-4244-6307-7

This paper addresses how to include EMC issues in risk assessment techniques. Part II discusses some general issues that are especially relevant to EMC, and Part III describes the details of incorporating EMC in risk assessments.

As Prof. Shuichi Nitta says in [17]: "*The development of EMC Technology taking account of systems safety is demanded to make social life stable.*" The author hopes that this paper makes a contribution to this work.

II. Relevant Risk Assessment Issues

A primer on hazards and risks

A HAZARD is anything with potential to do HARM, and the hazard level is derived from the type of harm and its severity. For example, a bladed machine can cause harm by cutting skin, flesh, even bone. We say it has a cutting hazard, and define its severity as being either minor, serious, or deadly (many other classifications being possible) depending on the maximum depth of cut and the parts of the anatomy exposed.

A hazard has a probability of occurrence. The RISK is the product of the hazard level, its probability of occurrence, and a factor that takes into account the observation that, when they occur, not all hazards result in the same harm, for example if there is the possibility of avoidance or limitation. (Risk level = {Hazard level} × {Probability of the hazard occurring} × {Possibility of hazard avoidance or limitation}).

Other multiplying factors can also be applied, and often are, for example we may decide that the risk level should vary according to social factors, such as the type of person, for example, small children, pregnant women, healthy adults, etc.

EMI does not affect hazards or their levels (ignoring the direct effects of EM fields on human health). However, EMI can affect the probability that hazards can occur, which is why it is important for achieving acceptably low risk levels.

Nothing can ever be 100% reliable, so there is always some risk. To insure that risks are not too high requires hazard analysis and risk assessment. This takes the information on a system's environment, design and application and – in the case of [3] – creates the Safety Requirements Specification, SRS (or its equivalent in other standards).

The SRS controls the design, realization, verification and validation of the safety system, to insure that risks are effectively controlled throughout the lifetime of the system.

Using risk assessment also helps avoid the usual project risks of over- or under-engineering the system.

The amount of effort and cost involved in the risk assessment should be proportional to the benefits required. These include: compliance with legal requirements, benefits to the users and third parties of lower risks (higher risk reductions) and benefits to the manufacturer of lower exposure to product liability claims and loss of market confidence.

Risk assessments are generally applied to simple systems

Modern control systems can be very complex, and are increasingly likely to be "systems of systems". If they fail to operate as intended, the resulting poor yields or downtimes can be very costly indeed.

Risk assessment – done properly – is a complex exercise in which competent and experienced engineers apply at least three different types of assessment technique to the entire system under review. To assess a complex system is a large and costly undertaking, so it is a good thing that it is not usually necessary.

The usual approach (e.g. [3]) – is to insure that the complex control system is competently designed, realized and maintained using proven good engineering practices – and then to assume that it will generally *not* be reliable enough to achieve effective control of the risks related to its use.

Instead, the safety of the overall control system is insured by a separate "safety-related system" – a much simpler system that can be risk-assessed quite easily. These systems often use "fail-safe" design techniques – when an unsafe situation is detected, the control system is overridden and the equipment under control brought to a condition that prevents or mitigates the harms that could occur.

For many types of industrial machinery, the safe condition is one in which all mechanical movement is stopped and hazardous electrical supplies isolated. A guard interlock is a typical example.

Such a fail-safe approach is useless in many life-support applications or anywhere where continuing operation-as-usual is the important issue, such as "fly-by-wire" aircraft.

However, even in situations where a guard interlock or similar fail-safe techniques cannot be used – and the control system is too complex for a practicable risk assessment – it is still generally possible to improve reliability by means of simple measures that can be cost-effectively risk-assessed.

A typical approach, for example, is to use multiple (redundant [18]) control systems with a voting system so that the majority vote is used to control the system. Alternatively, control might be switched from a failing control system to another that is not failing. For example, the Space Shuttle uses a voting system based on five computers [19].

Specifying the acceptable risk level

How low does the risk need to be? Nothing can ever be perfectly risk-free or safe, so it is necessary – for each hazard that exists – to specify the level of its risk that is at least broadly acceptable. [20] and [29] provide very useful guidance on what risks are broadly acceptable, and what may be tolerable under some circumstances.

Acceptable risk levels are culturally defined, and not amenable to mathematical calculation. They must be specified before the design process starts. The engineering principle of establishing an acceptable risk level and then designing to achieve it is enshrined in the functional safety standards [3], [12], [13] and others, and is a very sound one:

- for manufacturers to maximize their return on investment over the short, medium and long terms;
- for engineers and organizations who wish to abide by the IEEE's ethical guidelines [21].

Acceptable risk levels for functional safety are generally pro-

Presented at the IEEE 2010 International Symposium on EMC, July 25-30, 2010, Fort Lauderdale, Florida, USA, ISBN: 978-1-4244-6307-7

vided by "Risk Charts" (or "Risk Graphs"), e.g. Annex D in Part 5 of [3], Annex D of [12], Section 7.4.5 of Part 3 of [13].

Reducing the risk from an identified hazard is performed by what [3] calls a "Safety Function". A given safety system might perform several safety functions, each reducing the risk of a different hazard.

[3] applies a SIL specification to each safety function, chosen according to the rules in [3] to achieve the specified risk level for the particular hazard being risk-reduced. So for example a safety system might provide three safety functions at SIL 2, and two safety functions specified at SIL 3.

Figures 1 and 2 show the reliability ranges covered by SILs, and were developed from Tables 2 and 3 of Part 1 of [3].

IEC 61508's SILs for "on demand" safety functions...

Safety Integrity Level (SIL)	Average probability of a dangerous failure of the safety function, "on demand" or "in a year*"	Equivalent mean time to dangerous failure, in years*	Equivalent confidence factor required for each demand on the safety function
4	$\geq 10^{-5}$ to $<10^{-4}$	$>10^{4}$ to $\leq 10^{5}$	99.99 to 99.999%
3	$\geq 10^{-4}$ to $<10^{-3}$	$>10^{3}$ to $\leq 10^{4}$	99.9 to 99.99%
2	$\geq 10^{-3}$ to $<10^{-2}$	$>10^{2}$ to $\leq 10^{3}$	99% to 99.9%
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to $\leq 10^{2}$	90 to 99%

*** Approximating 1 year = 10,000 hrs of operation**

"Failure" includes any error, malfunction or fault that causes a hazard

Figure 1 Safety systems that operate "upon demand"

Examples of safety functions that operate on-demand include the braking system of an automobile, and guard interlocks in industrial plant. Most of the time they are doing nothing, but when operated (called a "demand on the safety function") they must do so with the required reliability.

IEC 61508's SILs for "continuous" safety functions...

Safety Integrity Level (SIL)	Average probability of a dangerous failure of the safety function per hour	Equivalent mean time to dangerous failure, in hours	Equivalent confidence factor required for every 10,000 hours of continuous operation
4	$\geq 10^{-9}$ to $<10^{-8}$	$>10^{8}$ to $\leq 10^{9}$	99.99 to 99.999%
3	$\geq 10^{-8}$ to $<10^{-7}$	$>10^{7}$ to $\leq 10^{8}$	99.9 to 99.99%
2	$\geq 10^{-7}$ to $<10^{-6}$	$>10^{6}$ to $\leq 10^{7}$	99% to 99.9%
1	$\geq 10^{-6}$ to $<10^{-5}$	$>10^{4}$ to $\leq 10^{5}$	90 to 99%

"Failure" includes any error, malfunction or fault that causes a hazard

Figure 2 Safety systems that operate continuously

Examples of safety functions that operate continuously include speed and/or torque control of automobiles and other vehicles, and of the motors in some machines and robots.

There is no requirement for a safety function to be provided by a single system, or to employ electronic technologies. In many situations mechanical protection such as bursting discs, blast walls, mechanical stops, etc. and management (such as not allowing people nearby during operation), etc., and combinations of them, can help achieve a safety function's SIL.

For example, a SIL 3 specified safety function requiring, say, 99.95% reliability, could be achieved by employing three independent protection methods, each one of which achieves just 99.65%. All three, two, just one, or none of these protection devices or systems could use electronic technology.

The use of non-electronic technologies to achieve the required SIL is the most powerful EMC design technique for achieving functional safety!

A philosophical point

Many EMC test professionals, faced with the information on hazards and risks above, say that because there is no evidence that EMI has contributed to safety incidents, the EMC testing that is done at the moment must be sufficient for safety.

However, the assumption that because there is no evidence of a problem, there *is* no problem, was shown to be logically incorrect in the 19th Century [22] and its use by NASA led directly to the Columbia space shuttle disaster [23].

[24] says: "*Lack of proof, or evidence, of risk should not be taken to imply the absence of risk.*"

Anyone who uses this argument is either poorly educated in matters of risk and risk reduction, or is hoping that the education of their audience is lacking in that area [25].

EMI problems abound [26], but it is unlikely that incidents caused by EMI will be identified as being so caused, because:

- Errors and malfunctions caused by EMI often leave no trace of their occurrence after an incident
- It is often impossible to recreate the EMI that caused the incident, because it was not recorded
- Software hides effects typically observed in analogue systems (e.g. EMI merely slows the data rate of Ethernet™, and blanks the picture on digital TV)
- Few first-responders or safety professionals know very much about EMI, much less understand it
- Accident data is not recorded in a way that might indicate EMI as a possible cause
- Accident investigations frequently overlook EMI possibilities, or treat EMC too simplistically

If a thorough risk assessment shows EMI *can* cause financial, mission or safety hazards, then undesirable incidents due to EMI *will occur*. If the probability of the incidents caused by EMI is higher than acceptable risk levels, their rate should be reduced until they are at least acceptable (i.e. risk reduction).

Hazards can be caused by multiple independent failures

It is often incorrectly assumed that only single failures need to be considered (so-called: "single-fault safety") – that the

Presented at the IEEE 2010 International Symposium on EMC, July 25-30, 2010, Fort Lauderdale, Florida, USA, ISBN: 978-1-4244-6307-7

simultaneous occurrence of two or more independent errors, malfunctions or other types of failure is just too improbable. Whether they are actually "too improbable" must be calculated, it cannot simply be assumed.

The number of independent failures that must be considered as happening simultaneously depends upon the required level of safety risk (or degree of risk reduction) and the probabilities of each independent failure occurring.

Not all failures are random

Many errors, malfunctions and other faults in hardware and software are reliably caused by certain EMI, physical or climatic events, or user actions. For example corrosion that degrades a ground bond or a shielding gasket after a time; an over-voltage surge that sparks across traces on a printed circuit board; a user who leaves a shielding panel open, etc.

These are "systematic" errors, malfunctions or other types of faults. They are not random, may be considered "built-in" and so *guaranteed to occur* whenever a particular situation arises. An example is shown in Figure 3.

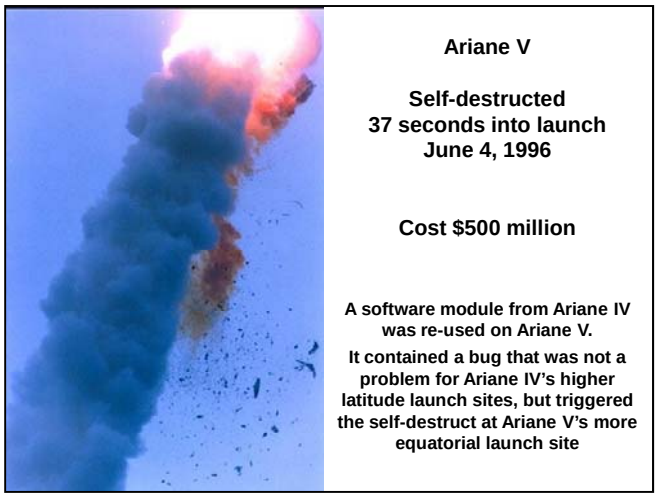

Figure 3 A systematic failure for Ariane V

[27] found that over 60% of major industrial accidents in the UK were systematic, i.e. were bound to happen eventually.

Not all failures are permanent

Many errors, malfunctions or other types of failure can be intermittent, for example:

- Poor electrical connections (a very common problem that can create false signals)
- Transient interference (conducted, induced, radiated)
- "Sneak" conduction paths caused by condensation, conductive dust, etc.

Failures that would be permanent might be recovered from, made transient, by error detection and correction or (after a much longer time) by a microprocessor watchdog re-booting the software, or (even longer) by manual power cycling.

"Common-Cause" errors, malfunctions and other failures

Two or more identical units exposed to the same conditions at the same time, for example:

- Ambient under or over-temperature
- Power supply under or over-voltage
- EM disturbances (conducted, induced, radiated, continuous, transient, etc.)
- Condensation, etc.

…will suffer the same systematic errors, malfunctions, etc. at the same time, called "common-cause" failures.

This means that using multiple redundant units [18] – a very common method for improving reliability to random errors, malfunctions or other types of failures – will not reduce risks of systematic failures when identical units, hardware or software are used to create the redundant system.

Devices can fail at two or more pins simultaneously

EMI can cause two or more pins on a semiconductor device, such as an integrated circuit (IC), to change state simultaneously.

An extreme example is "latch-up" – when all output pins simultaneously assume uncontrolled fixed states. This is caused by high temperatures, ionizing radiation and over-voltage or over-current on any pin of an IC. The presence of any one of the three causes increases an IC's susceptibility to latch-up due to the other two.

However, traditional risk analysis methods (e.g. FMEA) have often been applied very simplistically to electronics. For example, assuming that only one IC pin can be in error at a time, and that it will either be high or low.

The author has seen (so-called) FMEA-based risk assessments on safety-critical electronics conducted by a major manufacturer that simply went through all of the ICs one pin at a time and assessed whether a safety problem would be caused if each pin was permanently stuck high or low. This was the sole failure mode identification method applied.

Risk assessments need multiple techniques, and expertise

No one risk assessment technique can ever give sufficient "failure coverage", so *at least* three different types should be applied to any design, and probably more:

- At least one "inductive" or "bottom-up" method such as FMEA or Event-Tree
- At least one "deductive" or "top-down" method such as Fault-Tree or HAZOP
- At least one "brainstorming" method such as DELPHI or SWIFT

No risk analysis methods have yet been developed to cover EMC issues, so it is necessary to choose which existing methods to use, and adapt them to deal with EMI. Successful adaptation requires competency, skills and expertise in both safety engineering and real-life EMC (not just EMC testing).

Reasonably foreseeable use/misuse

It should never be assumed that an operator will always follow the Operators Manual (including when panicking), or would never do something that was just "too stupid".

Assessing reasonably foreseeable use or misuse requires the

Presented at the IEEE 2010 International Symposium on EMC, July 25-30, 2010, Fort Lauderdale, Florida, USA, ISBN: 978-1-4244-6307-7

use of “brainstorming” techniques by experienced personnel, and can achieve better “failure coverage” by including operators, maintenance technicians, field service engineers, etc.

Two Risk Assessment stages are required

When creating the SRS (or equivalent) only system block diagrams are likely to exist, so detailed risk analysis methods such as FMEA, FMECA, etc., cannot be applied. However, there are many other methods that may be used, and many of them are listed in 3.7 of [7]. At such an early stage in a project, only an “Initial Risk Assessment” is possible, so this is done and used to help create the SRS.

During the design, development, realization and verification phases of the project, detailed information becomes available on all of the mechanics, hardware and software. Appropriate risk analysis methods are applied to this design information – as it becomes available – to guide the project in real-time, to achieve the overall goals of the Initial Risk Assessment.

The Initial Risk Assessment is always carried out without considering the effects of any risk controls that are in place, or may be considered for each hazard. Without assessing the uncontrolled risk, there is no way to determine if it has been reduced adequately, and to what degree of risk the user will be exposed should the control measures fail.

As the project progresses the Initial Risk Assessment accumulates more depth of analysis, eventually producing the Final Risk Assessment at the end of the project

The Final Risk Assessment is a very important part of the safety documentation of a project, and can only be completed when the project has been completed. The real value of it lies in the process of developing it *during* the project, to achieve the acceptable risk levels (or risk reductions) whilst also saving cost and time (at least not adding significantly to them).

III. Incorporating EMC issues in Risk Assessments

The specifications on the foreseeable lifetime EM environment(s) are inputs to the risk analysis process, to help establish the risk level. Since environmental exposure and user actions and misuse can degrade EM characteristics, their lifetime assessments are also inputs to the risk analysis.

Many foreseeable failures occur simultaneously, for example:

- Two or more strong radio channels (especially near two or more cellphones, walkie-talkies, or a base-station or broadcast transmitter)
- One or more radiated RF fields plus distortion of the mains power supply waveform
- One or more radiated RF fields plus an ESD event
- A distorted mains waveform plus a mains dip, dropout, short interruption, transient or surge
- A power supply over-voltage transient plus conductive condensation
- One or more RF fields plus corrosion or wear that degrades enclosure shielding effectiveness
- One or more RF fields plus a shielding panel left open by the user
- Conducted RF on the power supply plus a high-impedance ground connection on the supply filter due to loosening of the fasteners that provide the bonding connection to the ground plane due to vibration, corrosion, etc.
- Power supply RF or transients plus filter capacitors that have, over time, been open-circuited by over voltages, and/or storage or bulk decoupling capacitors that have lost much of their electrolyte due to time and temperature.

Hundreds more examples could be given, and all reasonably foreseeable events and combinations of them must be considered by the risk assessment.

Intermittent contacts, open or short circuits, can cause spurious signals like some kinds of EMI, and are significantly affected by the physical/climatic environment over the lifetime. One example of this kind of effect is contact resistance modulated by vibration. This effect is called “vibration-induced EMI” by some.

EMI and intermittent contacts can – through direct interference, demodulation and/or intermodulation [8] – cause “noise” to appear in any conductors that are inadequately protected against EMI. “Noise” can consist of degraded, distorted, delayed or false signals or data, and/or damaging voltage or current waveforms.

Where “top down” or deductive risk analysis methods such as Fault Tree Analysis are used, they must take into account that significant levels of such noise can appear at any or all signal, control, data, power or ground ports of any or all electronic units – unless the ports are adequately protected against EMI. For radiated EMI, the unit’s enclosure is considered a port.

The noises appearing at different ports and/or different units could be identical or different, and could occur simultaneously or in some time-relationship to one another.

Where “bottom-up” or inductive (also called causative) risk analysis methods such as FMEA are used, the same noise considerations as above apply. In this case, the noise can appear at any or all pins of any or all electronic devices on any or all printed circuit boards (PCBs) in any or all electronic units – unless the units are adequately protected against EMI.

Similarly, the noises appearing at different pins or different devices, PCBs or units could be identical or different, and could occur simultaneously or in some time relationship.

It is often quite tricky to deal with all possibilities for EMI, physical, climatic, intermittency, use, misuse, etc., which is why competent “EMC-safety” expertise should always be engaged on risk assessments, to help insure all reasonably foreseeable possibilities have been thoroughly investigated.

The good news is that appropriate design techniques can deal with the many possibilities for EMI to cause errors, malfunctions or other types of fault. Risk analysis techniques determine if they are a) needed, and b) effective.

Presented at the IEEE 2010 International Symposium on EMC, July 25-30, 2010, Fort Lauderdale, Florida, USA, ISBN: 978-1-4244-6307-7

IV. Conclusions

Trying to achieve the reliability levels required by the SILs in [3], or similar low levels of financial or mission risk means that any practicable EMC testing regime can only take us part of the way to achieving our goals.

Risk assessment is a vital technique for controlling and assessing EMC design engineering, but since no established risk analysis techniques have yet been written to take EMI into account, it is necessary for experienced and skilled engineers to adapt them for that purpose.

This paper has provided some initial guidance, and it is to be hoped that others, more expert than the author, will develop this new area of "EMC risk assessment" in coming years.

Acknowledgment

Many thanks to Doug Nix for improving the text on safety.

References

[1] IEC/ TS 61000-1-2, Ed.2.0, 2008-11, "Electromagnetic Compatibility (EMC) – Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena", an IEC basic safety publication, http://webstore.iec.ch

[2] Marcel Van Doorn, "Towards an EMC Technology Roadmap", Interference Technology's 2007 EMC Directory & Design Guide, pages 182-193, www.interferencetechnology.com

[3] IEC 61508 (in seven parts), "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems", IEC basic safety publication, http://webstore.iec.ch

[4] Ron Brewer, "EMC Failures Happen", Evaluation Engineering magazine, December 2007, available: www.evaluation engineering.com/features/2007_december/1207_emc_test.aspx

[5] Keith Armstrong, "Why EMC Immunity Testing is Inadequate for Functional Safety", 2004 IEEE International EMC Symposium, Santa Clara, August 9-13, ISBN 0-7803-8443-1, pp 145-149. Also: Conformity, March 2005, available: www.conformity.com/artman/publish/printer_227.shtml.

[6] Keith Armstrong: "EMC for the Functional Safety of Automobiles – Why EMC Testing is Insufficient, and What is Necessary", 2008 IEEE International EMC Symposium, Detroit, August 18-22, ISBN 978-1-4244-1699-8 (CD-ROM)

[7] The IET, "EMC for Functional Safety", Edition 1, August 2008, available: www.theiet.org/factfiles/emc/emc-factfile.cfm or www.emcacademy.org/books.asp

[8] Keith Armstrong, "Why Increasing Immunity Test Levels is Not Sufficient for High-Reliability and Critical Equipment", 2009 IEEE International EMC Symposium, Austin, TX, August 17-21, ISBN (CD-ROM): 978-1-4244-4285-0

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

[10] IET, "Computer Based Safety-Critical Systems", Sept. 2008, available: www.theiet.org/factfiles/it/computer-based-scs.cfm?type=pdf

[11] Alexandre Boyer *et al*, "Characterization of the Evolution of IC Emissions After Accelerated Aging", IEEE Trans. EMC, Vol. 51, No. 4, November 2009, pages 892-900

[12] ISO 14971 Ed.2, "Medical devices – Application of risk management to medical devices", www.iso.org

[13] Draft ISO 26262 (10 parts), Road vehicles – Functional safety, www.iso.org

[14] Keith Armstrong, "Specifying Lifetime Electromagnetic and Physical Environments – to Help Design and Test for EMC for Functional Safety", 2005 IEEE International EMC Symposium, Chicago, August 8-12, ISBN: 0-7803-9380-5

[15] Keith Armstrong, "Design and Mitigation Techniques for EMC for Functional Safety", 2006 IEEE International EMC Symposium, Portland, August 14-18, ISBN: 1-4244-0294-8

[16] Keith Armstrong, "Validation, Verification and Immunity Testing Techniques for EMC for Functional Safety", 2007 IEEE International EMC Symposium, July 9-13, Honolulu, ISBN: 1-4244-1350-8

[17] Prof. Shuichi Nitta, "A Proposal on Future Research Subjects on EMC, From the Viewpoint of Systems Design", IEEE EMC Society Newsletter, Special 50th Anniversary Section: "The Future of EMC and the EMC Society", Issue 214, Summer 2007, pages 50-57, http://www.emcs.org.

[18] "Redundancy (engineering)", available: http://en.wikipedia.org/wiki/Redundancy_(engineering)

[19] "IBM and the Space Shuttle", available: www-03.ibm.com /ibm/history/exhibits/space/space_shuttle.html

[20] "Reducing Risks, Protecting People – HSE's Decision-Making Process", The UK Health & Safety Executive, ISBN: 0-7176-2151-0, www.hse.gov.uk/risk/theory/r2p2.pdf

[21] "IEEE Ethical Code of Practice", The IEEE, available: http://temp.onlineethics.org/codes/IEEEcode.html

[22] Dr. Antony Anderson's presentation to the 20th Conference of the Society of Expert Witnesses, Alexander House, Wroughton, UK, May 16, 2008, www.sew.org.uk, www.antony-anderson.com.

[23] Prof. Henry Petrowski, "When Failure Strikes", New Scientist, July 29, 2006, page 20, available: www.newscientist.com/channel/opinion/mg19125625.600 -the-success-that-allows-failure-to-strike.html

[24] Felix Redmill, "Making ALARP Decisions", Safety-Critical Systems Club Newsletter, Vol. 19, No. 1, Sept, 2009, pages 14-21, www.safety-club.org.uk

[25] Keith Armstrong, "Absence of proof is not proof of absence", The EMC Journal, Issue 78, September 2008, pp 16-19, available from the archives at www.theemcjournal.com

[26] "The First 500 Banana Skins", Nutwood UK, Oct. 2007, a compendium of anecdotes, reports, etc., on EMI incidents, from www.emcacademy.org/books.asp (or read on-line at www.theemcjournal.com)

[27] "Out of Control – Why Control Systems Go Wrong and How to Prevent Failure", The UK Health & Safety Executive, ISBN: 0-7176-2192-8, available: www.hse.gov.uk/pubns/priced/hsg238.pdf

[28] "Ariane V", available: http://en.wikipedia.org/wiki/Ariane_5

[29] "The Tolerability of Risk from Nuclear Power Stations", The UK Health & Safety Executive, available: www.hse.gov.uk/nuclear/tolerability.pdf.