IEEEemcsymp2016

CCC

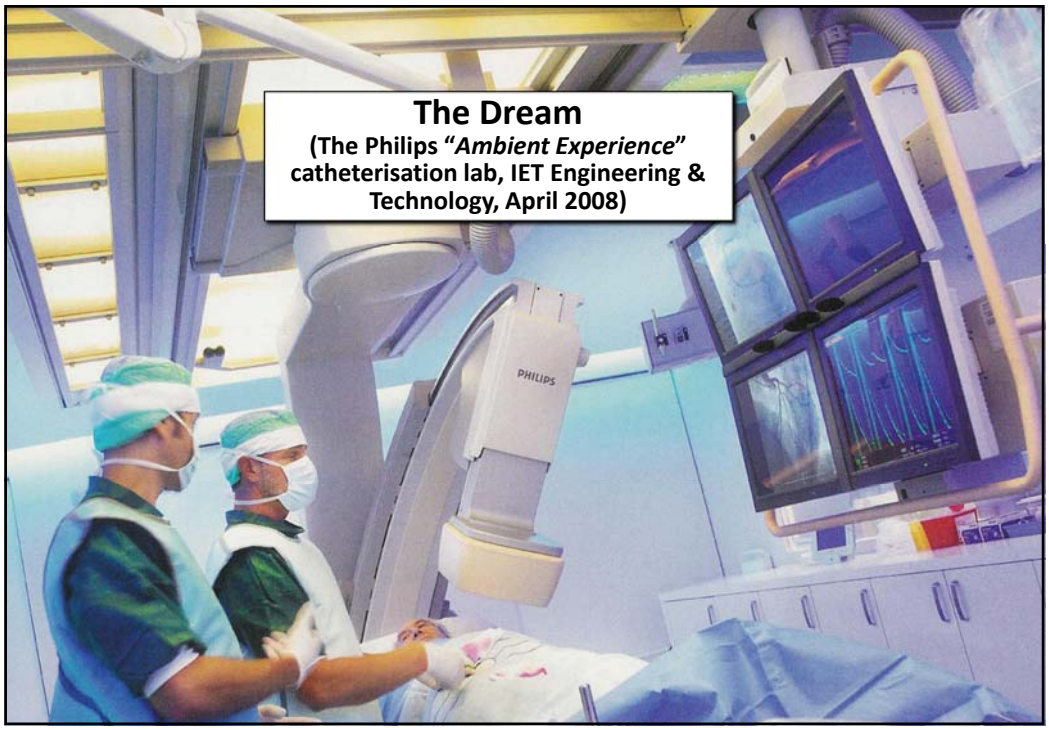
Ottawa Tutorial FRI-AM-2

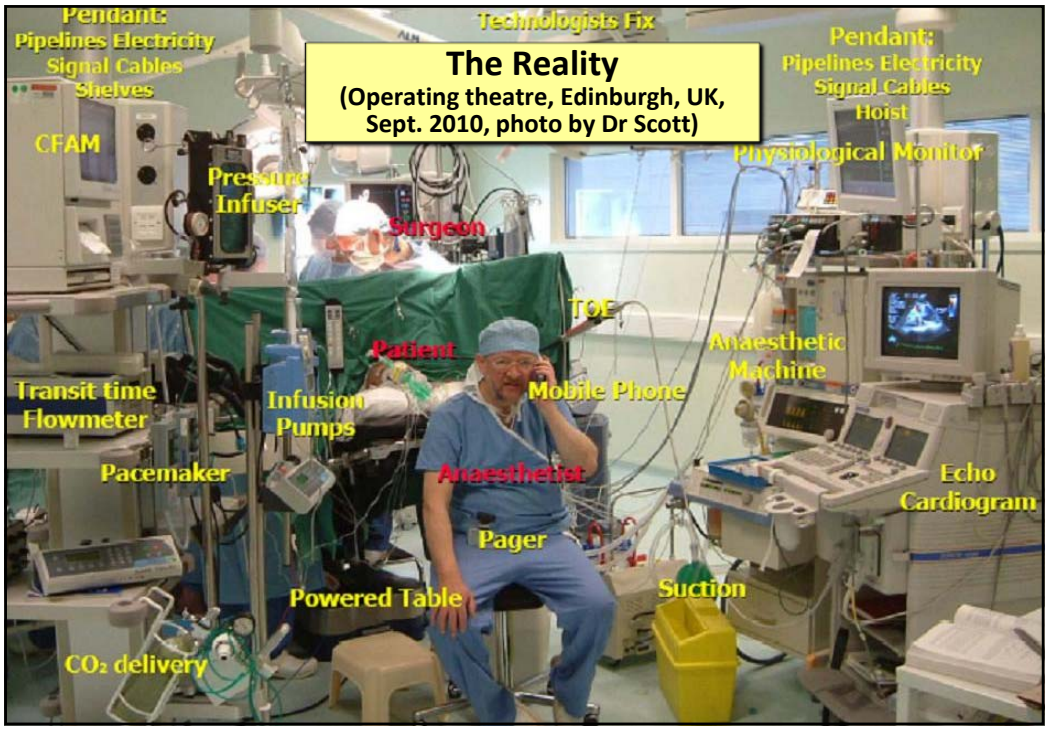
Introduction to Medical EMC

Risk Management of Electromagnetic Disturbances

Keith Armstrong, EurIng, CEng, FIET, Senior MIEEE, ACGI
phone & fax: +44 (0)1785 660 247
keith.armstrong@cherryclough.com
www.cherryclough.com

CHERRY CLOUGH CONSULTANTS LTD





CCC

Contents

- Introduction to Functional Safety
- ISO 14971 versus IEC 61508
- Risk Management of EM Disturbances in IEC 60601-1-2:2007
- EMC Immunity Testing: Deficiencies for Risk Management
- Risk Management of EM Disturbances in IEC 60601-1-2:2014
- The First *Practical* Approach to Risk-Managing EM Disturbances

Introduction

- **Where errors, malfunctions or failures in digital systems could cause increase safety risks…**
  - **the new safety engineering discipline Functional Safety was created to ensure that such risks stay low enough**
- **Increasingly complex electronic hardware and software is increasingly being used in increasing numbers of devices, equipment and systems…**
  - **all electronics can suffer EMI (electromagnetic interference) when their signals and/or power are degraded by EM disturbances in their environment…**
  - **so Functional Safety has to take EM disturbances fully into account as one of many causes of risk**

ISO 14971 versus IEC 61508 (1)

- **IEC 61508 is the basic IEC standard on Functional Safety…**
  - **and requires the use of an audited Risk Management (RM) process to ensure that functional safety risks will remain acceptable over the entire lifecycle**
- **All IEC product, product-family and generic standards that address functional safety risks must be based on IEC 61508's requirements…**
    - **in accordance with the IEC's rules…**
  - **however, IEC's SC 62A requested, and was permitted, to use ISO 14971 instead for all medical safety standards**

ISO 14971 versus IEC 61508 (2)

- IEC 61508 is a very large document…
  - most of it being a comprehensive guide on the use of well-proven, practical, Techniques & Measures (T&Ms)…
  - for system, hardware and software design, and their verification and validation…
  - to be able to demonstrate to an independent assessor that a safety-related system's functional safety risks will remain acceptably low…
  - over that system's entire lifecycle

ISO 14971 versus IEC 61508 (3)

- ISO 14971 has overall Risk Management (RM) principles that are pretty much in line with the Functional Safety requirements in IEC 61508...
  - so we can say that ISO 14971's Risk Management ≡ IEC 61508's Functional Safety
- BUT ISO 14971 provides *no practical guidance whatsoever*…
  - on how to ensure that safety risks caused by errors, malfunctions or faults in digital systems remain acceptably low over an entire lifecycle

Requirements for Risk Managing EM Disturbances in IEC 60601-1-2:2007 (1)

- IEC 60601-1-2 Ed.3:2007 requires achievement of 'ESSENTIAL PERFORMANCE' (which it doesn't define!)
  - ESSENTIAL PERFORMANCE is defined in IEC 60601-1 Ed 3.1:2012 subclause 3.27 as the: 'performance of a clinical function, other than that related to BASIC SAFETY, where loss or degradation beyond the limits specified by the MANUFACTURER results in an unacceptable RISK'
  - subclause 3.102 defines RISK as the: 'combination of probability of occurrence of HARM and the SEVERITY of that HARM'
- Because RM of EM disturbances is not an explicit requirement in 60601-1-2:2007…
  - many manufacturers and their Test Labs *incorrectly assume* that all they have to do is pass EMC tests!

Requirements for Risk Managing EM Disturbances in IEC 60601-1-2:2007 (2)

- IEC 60601-1-2 Ed.3:2007 has no guidance on how to actually *do* RM of EM disturbances…
  - although it's Bibliography lists the IEC's basic publication on EMC for Functional Safety, IEC TS 61000-1-2:2008…
  - unfortunately, applying IEC TS 61000-1-2:2008 is difficult because it uses IEC 61508's terminology – which does not correspond at all with ISO 14971…
    - the IET's 2008 Guide on EMC for Functional Safety uses ordinary English engineering language to describe how to comply with 61000-1-2:2008, available for free from: www.theiet.org/factfiles/emc/emc-factfile.cfm…
    - *but this was discovered in 2010 to be impractical, see later*

EMC Immunity Testing: Deficiencies for Risk Management (1)

- **No practicable EMC Test Plan could prove that risks due to EM disturbances were acceptably low…**
  - **because it would have to cover *all reasonably foreseeable*…**
    - **maximum EM disturbances over the entire lifecycle (normal test standards cover 80-90% of typical, in a week)…**
    - **physical and climatic stresses, aging, wear, corrosion, misuse, etc…**
    - **degradations/faults in EM mitigation and circuits, simulated individually, and foreseeable combinations…**
    - **angles of incidence, polarisations, modulation types and frequencies, transient waveshapes and rep. rates, etc…**
    - ***and foreseeable combinations of all of the above!***

EMC Immunity Testing: Deficiencies for Risk Management (2)

- **Digital systems are non-linear…**
  - **meaning that, unlike (linear) analog systems, no amount of testing can predict the behaviour of the untested digital states that remain…**
  - **but testing all possible combinations of perfectly correct inputs to a digital system can easily take millions of years, even using the fastest test systems available…**
  - **so a common problem with digital systems is *failures due to untested combinations of correct inputs*, see: https://en.wikipedia.org/wiki/Robustness_(computer_science)**
  - **also making it is impossible to prove a digital system is safe enough simply by testing, e.g. for EM immunity**

EMC Immunity Testing: Deficiencies for Risk Management (3)

- There are at least two other good reasons why immunity testing cannot be sufficient on its own to prove that safety risks are low enough…
  - if you need more information, I will be happy to provide conference papers and magazine articles that describe these issues in great detail…
    - including papers I have presented at:
      IEEE EMC International Symposia;
      IEEE PSES International Symposia;
      EMC-Europe International Symposia;
      IEE International System Safety Symposia,
      Safety-Critical Systems Symposia…
    - every year from 2004 to 2016

Requirements for Risk Managing EM Disturbances in IEC 60601-1-2:2014 (1)

- Unlike IEC 60601-1-2:2007…
  - IEC 60601-1-2 Ed.4:2014 includes many normative requirements and much informative guidance on Risk Managing electromagnetic disturbances…
    - all based on the IET's 2008 Guide, which it lists as an Informative Annex for more detailed advice on how to comply
    - *which was discovered in 2010 to be impractical!*
    - *see later for a practical method published in 2013, which was unfortunately too late for inclusion in Ed.4:2014*

Requirements for Risk Managing EM Disturbances in IEC 60601-1-2:2014 (2)

- The manufacturer documents what he has done about Risk Managing his product's responses to EM disturbances over its expected service life…
  - in a RISK MANAGEMENT FILE…
    - which will also describe the Risk Management activities he has undertaken for compliance with IEC 60601-1 and other 60601-x standards
- Compliance will depend on the assessment of this file by the relevant safety assessor (an EU Notified Body, the FDA, etc.)…
  - and not merely on the EMC test results *(which can never be sufficient to prove low-enough risks, see earlier)*

Requirements for Risk Managing EM Disturbances in IEC 60601-1-2:2014 (3)

- It is important to understand that:
  a manufacturer's RM activities cannot be performed by an EMC Test Laboratory
- The EMC Test Lab can check that the RM requirements have actually been followed…
  - but cannot actually *perform* them (that's the Manufacturer's responsibility)…
  - or verify/validate their compliance (that's the Notified Body's or FDA's responsibility)

Requirements for Risk Managing EM Disturbances in IEC 60601-1-2:2014 (4)

- Ed.4:2014 is *only* about Risk Management of EMC, for which it includes specific requirements…
  - it includes EMC immunity tests that *look similar* to those in previous Editions, *but are different*…
    - because their PASS Performance Criterion is that Basic Safety and Essential Performance are both maintained during and after the immunity tests…
    - even if achieved at the expense of Performance, e.g. if the equipment/system stops working!
- "Ordinary EMC compliance" for medical devices now needs the application of IEC TR 61000-4-2:2016…
  - as it is no longer covered under IEC 60601-1-2

Requirements for Risk Managing EM Disturbances in IEC 60601-1-2:2014 (5)

- Like Ed.3:2007, Ed.4:2014 includes EMC tests that cover the commonplace EM disturbances…
  - but all *reasonably foreseeable* EM disturbances must be considered by the Risk Assessment…
  - and, if significant, taken into account in the EMC design…
    - and then also taken into account by the design verification and validation…
  - using at least one of a variety of appropriate methods…
    - e.g. expert design review, testing, etc.

Requirements for Risk Managing EM Disturbances in IEC 60601-1-2:2014 (6)

- **Basic Safety and Essential Performance must be maintained throughout the Expected Service Life in the EM environment(s) of the intended use…**
  - **so all ageing, wear, corrosion, etc. issues must be taken into account in the Risk Assessment…**
  - **and must also be taken into account in the EMC design and its verification/validation…**
    - ***for this reason I recommend simulating the worst case environmental conditions over the life on an example of the medical equipment (e.g. using HALT test methods)…***
    - ***re-checking the EMC performance results on the 'aged' unit***

Requirements for Risk Managing EM Disturbances in IEC 60601-1-2:2014 (7)

- **Risk Analysis should take account of effects on emissions/immunity of reasonably foreseeable:**
  - **a) Faults**
  - **b) EM disturbances, including the actual modulation frequencies that can occur in the use environment(s)**
  - **c) Physical and climatic phenomena**
  - **d) Use and misuse…**
  - **– and reasonably foreseeable simultaneous combinations of any/all of the above..**
  - ***– although not a normative requirement in Ed.4:2014, I recommend it be treated as if it is, because it is a normative requirement in the basic IEC publication – IEC TS 61000-1-2:2008***

Requirements for Risk Managing EM Disturbances in IEC 60601-1-2:2014 (8)

- Ed.4:2014's Informative Annex F gives additional guidance on RM of EM disturbances…
  - and refers to 61000-1-2 Ed.2:2008 and the IET's 2008 Guide on it…
  - although Ed.4:2014 is not a complete application of basic IEC publication IEC TS 61000-1-2 Ed.2:2008
  - *so I recommend taking full account of all the NOTES in its normative text and all of the informative text in its Annex F…*
  - *but even so, we now know it is not a practical approach – see the next section*

The first *practical* approach to Risk Managing EM Disturbances (1)

- By 2010, experiences of trying to apply IEC TS 61000-1-2:2008 or the IET's 2008 Guide were…
  - there were too few EMC engineers willing/able to specify a future EM environment (and perhaps it is impractical to even *try* to do this)…
    - or to design EM filtering, shielding, surge suppression, etc. that would be reliable enough over a lifecycle…
  - and too few EU Medical Notified Bodies who can do any more than review EMC test reports…
  - and academia and industry had no interest in developing the necessary competencies

The first practical approach to Risk Managing EM disturbances (2)

- So, starting in 2010, the IET's Working Group on EMC for Functional Safety developed new guidance…
  - published August 2013 as: "Overview of techniques and measures related to EMC for Functional Safety"…
  - already included in IEC 61000-1-2:2016 as Annex B…
  - accepted as a replacement for Annex F in Amendment 1 to IEC 60601-1-2 Ed.4:2014 (due 2019)…
  - being published by IET Standards in 2016/2017 as the "IET Code of Practice on Electromagnetic Resilience"…
  - and being developed for publication in 2018 as the IEEE Standard on "Techniques and Measures for the Risk Management of Electromagnetic Disturbances"

The first practical approach to Risk Managing EM disturbances (3)

- The IET's 2013 guidance is (very briefly) as follows:
  - either use the 'Big Grey Box' approach…
  - high-spec, rugged EM mitigation (i.e. shielding, filtering, suppression) familiar from military projects…
  - or use well-proven design, verification and validation T&Ms to achieve sufficient 'EM Resilience'
  - *the IET's 2013 guidance: "Overview of techniques and measures related to EMC for Functional Safety" is free from: www.theiet.org/factfiles/emc/emc-overview.cfm*

‘Big Grey Box’ examples

The first practical approach to Risk Managing EM disturbances (4)

- **The IET Working Group determined which 61508 T&Ms had benefits for EMC, and developed them to be capable of providing EMI Resilience, essentially…**
  - **hardware / software reliably detects the effects of EMI…**
    - **i.e. EM disturbances that exceed the protection provided by the EM mitigation…**
  - **and takes appropriate actions (as described in a Safety Case) to maintain risks at acceptable levels…**
    - **for example by switching the system to a ‘Safe State’…**
    - **or correcting for effects of the EMI (e.g. by switching control to a backup system that is unaffected by the EMI)**

CCC

The first practical approach to Risk Managing EM disturbances (5)

- '61508 Industry' Functional Safety designers and assessors are very experienced with T&Ms…
  - which are all concerned with making systems, hardware and software more resilient to the effects of errors, malfunctions, faults, etc.
- The IET's new guidance details which of 61508's T&Ms are good for EM Resilience…
  - and how to modify some of them to make them more effective for EMI…
  - which won't require them to learn much more

CCC

The first practical approach to Risk Managing EM disturbances (6)

- It is possible to rely ***solely*** on 61508's T&Ms to create functionally safe systems…
  - but they can suffer too much downtime, i.e. have unacceptably low availability, as EMI causes them to switch to a Safe State, too often
- Such systems can be expected to be modified by users or owners to improve availability…
  - any subsequent dangerous failures would be *the manufacturer's fault*…
  - because such misuse is reasonably foreseeable

The first practical approach to Risk Managing EM disturbances (7)

- **Adequate availability simply needs compliance with the normal EMC emissions/immunity test standards…**
  - **for both the application and its EM environment(s)…**
  - **the EMC community has (of course) great experience with doing exactly this…**
  - **the new thing in the IET's new guide, is that this EMC compliance should be maintained throughout the whole lifecycle…**
  - **which won't require EMC engineers to learn much more, either**

The first practical approach to Risk Managing EM disturbances (8)

Compliance with the usual, relevant EMC standards for functionality – over the complete lifecycle

'EMC-improved' IEC 61508 design T&Ms reduce the residual risks to the extent required

Overall result: EMI Resilience

EM disturbances should not create unacceptable Functional Safety risks, over the lifecycle

Good EMC engineering practices used at all levels of design

The *normative* RM requirements in IEC 60601-1-2 Ed.4:2014

- Clause 4.1: Overall requirement to apply RM (to ISO 14971)
- Clause 8.1: Assess the EM environment (EME) and apply other immunity tests if necessary
- Clause 8.9: Base RM & testing on predicted EME + any mitigation; plus assess reliability of EM mitigation
- Clause 8.9, Table 4 (Enclosure port): Risk assess whether to use different modulations in radiated immunity tests
- Clause 8.9 Tables 5 (Power port); 6 (DC port); 7 (Patient port); 8 (SIP/SOPs): Risk assess whether to use different modulations in the conducted immunity tests
- Clause 8.10 Assess new/other wireless comm's services; plus likelihood of close proximity of mobile devices, and expanding radiated immunity tests as appropriate

How the IET's 2013 approach deals with Ed.4's RM requirements (1)

- Clauses 8.1, 8.9, and 8.10 assess the ME's future EM Environments (so that immunity tests & levels are relevant)…
  - plus assess whether the ME has special susceptibilities, (so that immunity tests use relevant modulations)
- Clause 8.9's RM requirements also try to foresee the degradations in EM performance over the expected service life…
  - from faults, aging, wear, corrosion, etc…
- All so that the risks that EM disturbances might cause EMI that causes a safety hazard can be kept low-enough by suitable design, testing and maintenance

How the IET's 2013 approach deals with Ed.4's RM requirements (2)

- **Unfortunately we *can't* perform these activities accurately-enough to ensure low-enough risks *over the expected service life***
- **So the IET "EM Resilience" approach *effectively* says:**
  - **assess the EM environment, including close proximity of mobile transmitters, etc…**
    - **then test accordingly to ensure no EM disturbances cause EMI in the ME *most of the time*…**
  - ***plus* use hardware, software and system T&Ms that detect *any/all EMI* in the ME *whatever their cause*…**
  - **and take appropriate actions to ensure that risks remain low-enough to comply with the overall RM requirement in Clause 4.1**

How the IET's 2013 approach deals with Ed.4's RM requirements (3)

- **All of these RM requirements can be solved by using the Big Grey Box approach…**
  - **so the 'EM Resilience' approach tends to be used when the Big Grey Box method is unsuitable…**
  - **usually for reasons of cost, size, and/or weight, but sometimes even because of its poor aesthetics**
- **The remaining normative RM requirements (in Clauses 4.2, 4.3.1, 8.5, 8.7, and Table 3,) are just 'plain' risk assessment issues…**
  - **having nothing to do with EM disturbances (other than being used within an EMC standard), and the IET 'EM Resilience' approach does not affect them**

CCC

Ottawa Tutorial FRI-AM-2
Introduction to Medical EMC

Risk Management of Electromagnetic Disturbances

the end

Keith Armstrong, EurIng, CEng, FIET, Senior MIEEE, ACGI
phone & fax: +44 (0)1785 660 247
keith.armstrong@cherryclough.com
www.cherryclough.com