Electrical and Electronic Safety in Medical Devices – Human Factors, Software and Electromagnetic Compatibility

a report by

Trevor Lewis *and* **Keith Armstrong**

1. Chartered Engineer and Member, Institution of Engineering and Technology (IET); and 2. Chairman, Working Group on 'EMC and Functional Safety', Institution of Engineering and Technology (IET)

Trevor Lewis is a Chartered Engineer and a member of the Institution of Engineering and Technology (IET) Mr Lewis is also a member the Institute of Physics and a Chartered Physicist. He has written and presented on many aspects of medical device business development both nationally and internationally, including two major management reports for the Financial Times.

EurIng Keith Armstrong chairs the the Institution of Engineering and Technology's (IET's) Working Group on 'EMC and Functional Safety' and is the appointed UK expert on the International Electrotechnical Commission (IEC) 61000-1-2 Electromagnetic Compatibility (EMC) and Functional Safety Committee.

First, Do No Harm!

The Greek physicians Hippocrates and Galen have both influenced modern so-called 'Hippocratic Oaths' that are often summarised as "first, do no harm!" This oath equally applies to those engaged in the worthy aim of bringing medical devices to market. A quote attributed to Hippocrates circa 415 BC is still applicable unchanged today:

"Life is short, science is lengthy, opportunity elusive, experience is dangerous, judgement is difficult."

The desire is to extend life and understand the science whilst securing the opportunity with benefits that outweigh the risks involved. This is the aim of modern medical device manufacturers and the purpose of much health technology assessment (HTA).

International Standards – A Sound Starting Point

Most countries around the world either use or base their electrical safety standards on those developed by the International Electrotechnical Commission (IEC). The key current standards for manufacturers of electrical or electronic medical devices to address are:

- EN 60601-1: 1990 "Medical electrical equipment. General requirements for safety" (IEC 60601-1: 1998 modified).
- PD IEC TR 62296: 2003 "Considerations of unaddressed safety aspects in the Second Edition of IEC 60601-1 and proposals for new requirements".
- IEC 60601-1-1: 2001 "Medical electrical equipment. General requirements for safety. Collateral standard. Safety requirements for medical electrical systems".
- IEC 60601-1-2: 2002 "Medical electrical equipment. General requirements for safety. Collateral standard. Electromagnetic compatibility. Requirements and tests".
- IEC 60601-1-4: 1996 "Medical electrical equipment. General requirements for safety. Collateral standard. General requirements for programmable electrical medical systems".
- IEC 60601-1-6: 2004 "Medical electrical equipment. General requirements for safety. Collateral standard. Usability".
- IEC 60601-1-8: 2003 "Medical electrical equipment. General requirements for safety. Collateral standard. General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems".
- ISO/IEC 62304: 2006 "Medical device software – Software life cycle processes".
- IEC 61508-3: 1998 "Functional safety of electrical/electronic/programmable electronic safety-related systems. Software requirements".

During late 2005 the IEC 60601-1 Third Edition Part 1: General requirements for basic safety and essential performance was published. It contains 786 pages (393 pages in the English-only version). This incorporates IEC 60601-1-4 and builds on all the 60601 series of standards. In the Foreword, p.21, it states that:

"Requirements in the electrical section have been further aligned with those for information technology equipment covered by IEC 60950-1 and a requirement for including a RISK MANAGEMENT PROCESS has been added."

The Introduction, on p.27 states that:

"This standard contains requirements concerning BASIC SAFETY and ESSENTIAL PERFORMANCE that are generally applicable to MEDICAL ELECTRICAL EQUIPMENT. For certain types of MEDICAL ELECTRICAL EQUIPMENT, these requirements are either supplemented or modified by the special requirements of a collateral or particular standard. Where particular standards exist, this standard should not be used alone."

There are numerous collateral and particular standards listed for medical devices and the harmonised standards notified in the Official Journal of the European Commission (OJEC) for the three main European Union (EU) Medical Devices Directives can be found at:
http://ec.europa.eu/enterprise/newapproach/standardization/harmstds/reflist.html

Checking the list for your particular medical device is a key action in determining appropriate electrical and electronic safety requirements in the EU. Whilst use of the standards is voluntary it is expected and sensible to use them. Applying these standards requires skilled and experienced engineers. As Hippocrates stated, experience is dangerous, but standards and laboratory testing can help avoid the worst situations from ever arising with a patient in a real situation. Judgement may sometimes be truly difficult but there is no excuse for not undertaking functional testing in a simulated environment where doing no harm can be guaranteed.

Designing for validation, applying appropriate quality system controls and comments on how far manufacturers should go in evaluating risks has been covered elsewhere by the authors.[1,2] If the harmonised standards and total quality management approach are rigorously implemented this should ensure safe medical devices, at least up to a point. The authors take the view that all too often this approach falls short of the real world experience and needs. The minimum aim must be electrical safety in all functional conditions. Functional safety includes – in the words of EN ISO 14971: 2001 Medical devices. Application of risk management to medical devices – taking into account reasonably 'foreseeable hazards', so that patients are not harmed in normal use in the real world, or where a single fault condition exists.

Usability, Human Factors and FDA

The IEC has produced the useful IEC 60601-1-6: 2004 Medical electrical equipment. General requirements for safety. Collateral standard. Usability that addresses the "usability engineering process". Usability, sometimes called Human Factors Engineering (HFE), is defined in this standard as the characteristic that "...establishes effectiveness, efficiency, and operator learnability and satisfaction." This is a risk-based process. The general guidance and rationales it annexes are useful. This is especially true of the 'contextual factors' that are addressed and the examples of user errors, abnormal use and design flaws. It includes comments on modelling the operator-equipment interface, has extensive reference documents listed and Annex EEE (informative) Sample Usability Specification is particularly useful as a checklist. It is complementary to the long established United States (US) Food and Drug Administration (FDA) guidance concerning environmental factors where humans use medical devices known as their 'Human Factors Program'. Please see: http://www.fda.gov/cdrh/humanfactors/

The benefits of HFE, according to the FDA Guide, are worth quoting:

- "Reduced risk of device use error;
- Better understanding of device status and operation;
- Better understanding of a patient's current medical condition;
- Easier to use (or more intuitive) devices;
- Reduced need for training;
- Reduced reliance on user manuals;
- Easier to read controls and displays;
- Safer connections between devices (i.e. power cords, leads, tubes, etc.);
- More effective alarms; and
- Easier repair and maintenance.

HFE (usability) should take place early in the product development process. It should include tools such as analysis of critical tasks, use error hazard and risk analysis, and realistic use testing."

The FDA guidance at this site is highly recommended and contains numerous further references.

A quoted Institute of Medicine report (1999), To Err Is Human – Building a Safer Health System, estimated that "...as many as 98,000 people die each year [in the USA] from medical errors in hospitals. This is more than the number who die yearly from motor vehicle accidents, breast cancer, or AIDS. Though many of these errors are not associated with medical devices, some are directly or indirectly related to medical device use."[3]

It is also worth quoting the identified human factors hazards that the authors believe should be considered when using EN ISO 14971:

- "Medical devices can be complex;
- Medical devices are often used under stressful conditions;
- Users may think differently than device designers do;
- Consumers now use devices that were originally designed for experienced medical personnel; and
- People blame repeated use errors on the user,

1. *Armstrong K, "Electromagnetic Compatibility for Functional Safety",* Business Briefing: Medical Device Manufacturing and Technology *(2005).*
2. *Lewis T, "Real World Issues – a trilogy",* Special Clinica Supplement *(May 2005) covering:*
   - *Existing products: how far should firms go to evaluate new risks?*
   - *Clinical trials or literature reviews? Get real or face stricter rules; and*
   - *Software in the Real World: how many bugs do you have?*
3. *To Err Is Human – Building a Safer Health System http://newton.nap.edu/html/to_err_is_human/*

rather than on poor product design or inadequate instructions for use, so people don't recognise the need for human factors."

Safety by Inherent Design for Intended Users in their Intended Environment Including Rare Events

Whilst very rare events, even if the consequences are fatal, can be considered a negligible risk by EN ISO 14971 it is worth learning from them and determining if the inherent design can be improved. This is consistent with the Medical Devices Directive 93/42/EC Annex I Essential Requirements I.' General Requirements that states:

"1. The devices must be designed and manufactured in such a way that, when used under the conditions and for the purposes intended, they will not compromise the clinical condition or the safety of patients, or the safety and health of users or, where applicable, other persons, provided that any risks which may be associated with their use constitute acceptable risks when weighed against the benefits to the patient and are compatible with a high level of protection of health and safety.

2. The solutions adopted by the manufacturer for the design and construction of the devices must conform to safety principles, taking account of the generally acknowledged state of the art. In selecting the most appropriate solutions, the manufacturer must apply the following principles in the following order:

- eliminate or reduce risks as far as possible (inherently safe design and construction),
- where appropriate take adequate protection measures including alarms if necessary, in relation to risks that cannot be eliminated,
- inform users of the residual risks due to any shortcomings of the protection measures adopted.

3. The devices must achieve the performances intended by the manufacturer and be designed, manufactured and packaged in such a way that they are suitable for one or more of the functions referred to in Article 1 (2) (a), as specified by the manufacturer.

4. The characteristics and performances referred to in Sections 1, 2 and 3 must not be adversely affected to such a degree that the clinical conditions and safety of the patients and, where applicable, of other persons are compromised during the lifetime of the device as indicated by the manufacturer, when the device is subjected to the stresses which can occur during normal conditions of use.

5. The devices must be designed, manufactured and packed in such a way that their characteristics and performances during their intended use will not be adversely affected during transport and storage taking account of the instructions and information provided by the manufacturer.

6. Any undesirable side-effect must constitute an acceptable risk when weighed against the performances intended."

IEC 60601-1-8: 2004 Medical electrical equipment. General requirements for safety. Collateral standard. General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems as listed earlier, is a Euro Norm (EN) standard but is not yet notified as a harmonised standard against any of the Medical Devices Directives. It represents the state of the art and is very much a human-factors centred document that discusses intelligent alarm systems' use. However, alarms are warnings, so the authors recommend that the application of this standard should come after inherently safe design risk mitigation or risk elimination have been progressed as far as is reasonably practical. It is strongly recommended that electrical/electronic systems should not rely on labelling or warnings for the safe use of the system.

The Report on the Expert Working Group on Alarms on Clinical Monitors, in response to Recommendation 11 of the Clothier Report: The Allitt Inquiry, provides useful insights arising from the malicious use of medical devices by a serial killer – Nurse Allitt.[4] This was published during early 1995 but sadly the lessons have still to be learnt by many medical device companies. If the lessons from the Expert Group on Alarms are applied and developed, electrical/electronic medical devices will be safer by 'inherent design'. This report should be seen as complementary to EN 60601-1-8. It is important, then, to list some of the key lessons for inherently safe design based in the section on 'Technical Issues'.

- Device design should aim to minimise false alarms.
- Where controls can be altered by movement they need to be lockable and only adjustable by a deliberate act.
- Where alarm settings are important their

4. *"The Report on the Expert Working Group on Alarms on Clinical Monitors in response to Recommendation 11 of the Clothier Report: The Allitt Inquiry",* Medical Devices Agency *(1995). This can be found at the UK's Medicines and Healthcare products Regulatory Agency (MHRA): http://www.mhra.gov.uk/home/idcplg?IdcService=GET_FILE&dID=798&noSaveAs=0&Rendition=WEB*

activation should be clear to users.
- The alarm should be appropriate to the environment and clinical need.
- Alarms for use in the home setting may require a different approach to the clinical setting.
- Data logging of critical functions should be considered to record when settings are changed so that malevolent interference is minimised.
- Alarms do need to be periodically checked and the important ones need to be available even after power failure.

Other parts of the report stress the need for a 'Procurement Checklist' that includes life-cycle management of devices and the appropriate 'Education and Training' of all users. What neither the report nor IEC 60601-1-8 addresses is user identification to ensure those actually operating the device are trained and authorised to do so. This is very much a 21st Century issue and the technology to do this by inherently safe design now exists. The importance of new technology was discussed in 2002 by Kent and Lewis, who raised the use of electronic signatures and electronic records.[5]

The FDA has issued guidance on Title 21 Code of Federal Regulations (21 CFR Part 11)

Electronic Records; Electronic Signatures that do include consideration of biometrics like fingerprints and retinal scans to determine who is using what and when, at least in quality systems but the association with device use seems natural and obvious to the authors.

Software Considerations

It has long been established that it is impossible to gain sufficient confidence that software will not cause unacceptable safety risks, by testing alone.[7] Well-proven safe software design techniques must be used as well as thorough testing. The FDA has long recognised that software, either stand-alone or embedded in devices, requires control during design, irrespective of device classification. The recent revision of the Medical Devices Directive (93/42/EEC)[8] also strengthens the regulatory expectations for software. This proposes to amend "Annex I Essential Requirements" to include:

"12.1a For devices which incorporate software or which are medical software themselves, the software must be validated according to the state of the art taking into account the principles of development lifecycle, risk management, validation and verification."

This statement is only surprising in the fact it needs to be made. Manufacturers should already be applying the 'state of the art' as given in paragraph two of "Annex I Essential Requirements". Medical device software development methodologies often lag behind the well-specified, controlled and structured methods used in other safety focused industries such as aerospace and automotive. These industries are also typically more sophisticated in their selection and use of appropriate tools for both requirements and software development that are fully CFR Part 11 compliant.

The FDA does have reasonable software guidance and the European regulators have undertaken some standards work concerning software as indicated in the list earlier.

The reason to use software tools for requirements and software development is simple: a faster time to market can be achieved. The resulting software is more reliable and more compliant with regulatory submissions. In a nutshell, it is more cost-effective and currently can be used as a competitive weapon against those who persist in the 'do it, fix it and keep fixing' type methodologies. Those who persist in such an antiquated approach will tell you it is faster. However, from the perspective of those who have experienced such software tools in use, those who keep spending development funds on fixing software in the field are like lumberjacks who do not have the time to sharpen their saws, think about which forest they are in or where and when the wood will be sold.

Provided software is well-specified in appropriate requirements documents and carefully selected software tools are used in development there is every possibility the resulting software will be inherently safer by design. Bugs and errors will also be easier to locate, trace through the system and fix cost-effectively.
The FDA's 2005 Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, makes it clear that

5. *Kent A & Lewis T, "Regulatory Trends and the Global Village",* Business Briefing: Medical Device Manufacturing and Technology *(2002).*
6. *"Title 21 Code of Federal Regulations (21 CFR Part 11) Electronic Records; Electronic Signatures", Please see: http://www.fda.gov/ora/compliance_ref/part11/*
7. *Musa, J D, Iannino A, and Okumoto K, "Software Reliability: Measurement, Prediction, Application", (1987) ISBN 0-07-044093-X, McGraw-Hill, New York.*
8. *"Proposal for a Directive of the European Parliament and of the Council amending Council Directives 90/385/EEC and 93/42/EEC and Directive 98/8/EC of the European Parliament and the Council as regards the review of the medical device directives", available from: http://ec.europa.eu/enterprise/medical_devices/revision_mdd_en.htm*

'traceabilityanalysis' is required for all devices that incorporate software no matter what their level of concern.[9] The following quote is a good summary of overall expectations:

"Verification 'means confirmation by examination and provision of objective evidence that specified requirements have been fulfilled.' 21 CFR 820.3(aa). In a software development environment, software verification is confirmation that the output of a particular phase of development meets all of the input requirements for that phase. Software testing is one of several verification activities intended to confirm that the software development output meets its input requirements. Other verification activities include;

- walk-throughs;
- various static and dynamic analyses;
- code and document inspections;
- module level testing;
- integration testing.

Design validation 'means establishing by objective evidence that device specifications conform with user needs and intended use(s).' 21 CFR 820.3(z)(2). Use of the term validation in this document is limited to design validation and does not include process validation as defined in 21 CFR 820.3(z)(1).

One component of design validation is software validation. Software validation refers to establishing, by objective evidence, that the software conforms with the user needs and intended uses of the device. Software validation is a part of design validation of the finished device. It involves checking for proper operation of the software in its actual or simulated use environment, including integration into the final device where appropriate. Software validation is highly dependent upon comprehensive software testing and other verification tasks previously completed at each stage of the software development life-cycle. Planning, verification, traceability, configuration management, and many other aspects of good software engineering are important activities that together help to support a conclusion that software is validated."

Other FDA guidance on software includes:

- General Principles of Software Validation; Final Guidance for Industry and FDA Staff (2002); and
- Guidance for Industry, FDA Reviewers and Compliance on Off-the-Shelf Software Use in Medical Devices (1999).

EMC for Functional Safety

Once the medical device, probably with lots of well-tested software, is assembled into a finished product it is good engineering practice to fully test it for safety and EMC. However, where electromagnetic interference (EMI) with electrical or electronic devices and/or with software could increase safety risks, EMC must be considered from the perspective of functional safety, which is quite different to doing EMC for compliance with EMC regulations. Just as for software, it is impossible to gain sufficient confidence that interference will not cause unacceptable safety risks, by testing alone – well-proven EMC design techniques must be used. The authors recommend a thorough evaluation of the foreseeable worst-case electromagnetic environment over the anticipated life-cycle to ensure the safety design takes it fully into account.[10,11] The laboratory tests should generally be to the 60601 series standards, although deviations may be needed to cover EMI that they do not (yet) cover, and a risk-based approach is expected. Particular identified threats should be closely studied and any problems solved in the laboratory, well before the device ever reaches the hands of its users.

The importance of taking EMC into account to achieve functional safety is hard to overstate, given the reliance of modern medical devices on electronics and software.1 The medical device or system must achieve the required electromagnetic performance robustly, and effective essential performance must be maintained, for all safety-related functions, over its anticipated life-cycle.

Post-Market Surveillance

All the above must be considered from the conceptual design stage with ever increasing technical scrutiny as the development process progresses but this does not stop at delivery of the device to the users. Post-market surveillance of devices working properly or incorrectly is a vital part of the overall design feedback and hence a part of Corrective Action Preventive Action (CAPA). An effective post-market surveillance procedure can help maintain the safety and effectiveness of both today's medical devices and those of the future. ■

9. *Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices (2005) http://www.fda.gov/cdrh/ode/guidance/337.html#3*
10. *Armstrong K, "Specifying Lifecycle Electromagnetic and Physical Environments – to Help Design and Test for EMC for Functional Safety", (2005)* IEEE International Symposium on EMC, Chicago*, Aug 8-12 2005, ISBN: 0-7803-9380-5, pp. 495–499.*
11. *Armstrong K, "Design and Mitigation Techniques for EMC for Functional Safety", (2006)* IEEE 2006 International Symposium on EMC, Portland, Oregon*, Aug 14-18 2006, ISBN: 1-4244-0294-8.*