International Standards and EU regulation of medical device software - an update

Sherman Eagles  
Partner, SoftwareCPR  
seagles@softwarecpr.com  
612-865-0107

Who am I?  
– 18 years at Medtronic, retired 2008  
– Last 10 years as a Medtronic Technical Fellow  
   working in area of software safety and reliability  
– Extensive work on standards related to medical device software  
– Convener of international standards working groups on medical device software  
– Now doing training and consulting on medical device software standards and software safety
What I’m going to talk about

– A brief overview of the European regulatory system – including use of harmonized standards
– Software in the medical device directives
– EN IEC 62304 – harmonized standard for medical device software life cycle processes
– IEC TR 80002-1 – software risk management
– IEC 80001-1 risk management for IT networks incorporating a medical device

Regulation in the European Union

• EU governing bodies issue directives to member countries
• Member countries must pass laws to implement the directives
• Competent authorities oversee the laws and accredit notified bodies
• Notified bodies determine if a product complies with the directive and issue a CE mark if it does
“New Approach” Directives

- Legislation identifies essential requirements in directives
- Only products fulfilling the essential requirements may be placed on the market
- Products that comply with harmonized standards are presumed to conform to the essential requirements

The medical device directives

- Active Implantable Medical Devices Directive (AIMD) - 1990
- Medical Devices Directive (MDD) - 1993
- In Vitro Diagnostic Medical Devices Directive (IVDD) - 1998
Software in the medical device directives

- Only reference in any of the essential requirements was to electrical programmable systems in the MDD
  Devices incorporating electronic programmable systems must be designed to ensure the repeatability, reliability and performance of these systems according to the intended use. In the event of a single fault condition (in the system) appropriate means should be adopted to eliminate or reduce as far as possible consequent risks.

Harmonized standard for electrical programmable systems

- IEC 60601-1-4
- After 2005 also 60601-1 3rd edition
2007 changes in directives

- Amendments to the MDD and AIMD were adopted by the EU parliament in 2007
- EU member countries have until March 2010 to implement the changes

Software changes in the 2007 amendments

- Same changes in both MDD and AIMD directives
- Clarified what software products may be medical devices
  - Software that is intended to be used specifically for diagnostic or therapeutic purposes is subject to the directive’s requirements.
Implications for software products

• Software products that are a single piece of software with an intended purpose that fits the medical device definition will be regulated as medical devices
  – This includes products that are not currently regulated

• A system that is a combination of software applications assembled for a purpose that fits the medical device definition may be regulated, but this is not yet clear.

Swedish report – June 2009


• Initiated and led by the Swedish Medical Products agency with involvement from users, manufacturers, standardization organizations and notified bodies in Sweden

• Task was to formulate a guideline for classification of medical information systems

• Concluded many medical information systems should be regulated as medical devices
Some products recommended for regulation

- Electronic medical record systems
- Anaesthetic record systems
- Patient data management systems
- Retinal imaging systems
- Radiological information systems
- Web based patient questionnaires
- Decision support systems
- ePrescription systems

Competent Authorities reaction

- Task force formed with Sweden chairing to draft guidance for regulation of software that meets the definition of a medical device
  - Sweden currently (until end of 2009) has the presidency of the EU
Joint CEN/CENELEC software group

• Currently under development
  – First meeting in June 2009

• Role
  – Monitor regulatory position related to software
  – Enable consistent approach to application of medical directives for software
  – Provide advice, proposals and suggestions to other EU bodies addressing software as a medical device
  – Ensure adequate standards are available

Software changes in the 2007 amendments

• Added a new essential principle
  ‘For devices which incorporate software or which are medical software in 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.’
Harmonization of IEC 62304

- November 2008, EN IEC 62304 was harmonized for software for MDD, AIMD and IVDD.
- No effective date given, but it is expected that notified bodies will require conformity by March 2010.

Role of standards in assuring safe medical device software

SAFE

All hazards have been addressed

Risks have been reduced to acceptable levels

Adequate process has been implemented (compliance with standards is often considered a demonstration of adequate process.)

Process is effective

ISO 14971
IEC 62304
AAMI TIR 32
IEC 60601-1
Status of IEC 62304

• Approved by both IEC and ISO as an international standard (joint development effort)
• Adopted by ANSI as a US national standard replacing ANSI/AAMI/SW 68
• Recognized by FDA for use in premarket submissions
• Harmonized in the EU under the MDD, AIMDD and IVDD
• Expected to be adopted by the Chinese SFDA

62304 philosophy

• Safe medical device software requires risk management, quality management and good software engineering
• Good software engineering requires critical thinking – can’t be done by checklist
• Manufacturers know more about their products than regulators
• The variety of medical devices requires a variety of approaches – one size does not fit all
• Resources should be used on what is important
• A standard should have minimum requirements, not best practices
IEC 62304 - What is it?

• A framework – processes, activities and tasks
  – Process is the top level, a process has activities and an activity has tasks. Specific requirements in IEC 62304 are generally at the task level.
• Identifies requirements for what needs to be done and what needs to be documented
• Specifies a software safety classification system
  – additional requirements apply as safety classification increases

IEC 62304 - What is not in it?

• Does not prescribe how to accomplish requirements
  – Not a “how to” with defined methods or practices
• Does not require a specific software life cycle
• Does not specify documents
  – What to document, not where it must go.

• All of these decisions are left to the manufacturer
IEC TR 80002-1

• IEC TR 80002-1:2009 Medical device software
  – guidance on the application of ISO 14971 to medical device software
• Gives guidance for each clause of 14971
• Status: approved
  – Will be published this fall

Software risk analysis

• In the system risk analysis, identify software items that could contribute to a hazardous situation
  – Direct control of hardware
  – Information that is used in diagnosis or treatment
• Identify potential causes of the software item contributing to a hazardous situation
Potential software causes

- Incorrect or incomplete specification of functionality
- Defects in the software functionality
- Failure or unexpected results from SOUP (OTS)
- Hardware or software failures that could result in unpredictable software operation
- Reasonably foreseeable misuse

Systematic errors – the probability problem

- Software defects are systematic errors
- Systematic failure - design errors that do not occur randomly and for which a probability of occurrence cannot be calculated
- FDA has taken the position that probability/likelihood for software errors cannot be stated.
- How do you show that the risk from software is acceptable?
## Acceptable risk

- May be able to estimate residual risk (after risk control measures have been applied) of harm occurring, even if software failure occurs
- If residual risk cannot be estimated, then
  - Focus on severity of consequences
  - Show use of all reasonably practical risk controls
  - Show that risk control measures implemented are effective
  - Show that risk control measures meet applicable standards and are “state of the art”

## State of the art – from ISO 14971

"State of the art" is used here to mean what is currently and generally accepted as good practice. Various methods can be used to determine "state of the art" for a particular medical device.

Examples are:
- standards used for the same or similar devices;
- best practices as used in other devices of the same or similar type;
- results of accepted scientific research.

State of the art does not necessarily mean the most technologically advanced solution.
IEC 80001-1 (under development)

- IEC 80001-1:20xx Application of risk management for IT-networks incorporating medical devices

What is the problem?

- Increasing drive toward heterogeneous networks
- Increasing deployment of devices in multi-vendor / multi-modality networking environments
- Increasing mix of medical device & I.T. technologies
- Systems of Systems Result in ... Unanticipated Emergent Behaviors!

! Wireless networks increase the problem because you can’t segregate networks by separate cabling
Joint Commission Alert

December 11, 2008 - Safely implementing health information and converging technologies

• As health information technology (HIT) and “converging technologies”—the interrelationship between medical devices and HIT—are increasingly adopted by health care organizations, users must be mindful of the safety risks and preventable adverse events that these implementations can create or perpetuate.

Who is needed to address the problem?

• Network integrators and maintainers
• Clinical engineers
• Medical device manufacturers
• Non-medical network technologies

None of these parties can address the problem alone, problem solution for networks incorporating medical devices must be shared in a partnership or federated model.
What properties need to be ensured?

Risk management should be applied to address the following key properties:

– safety;

– effectiveness (effective treatment of the patient using the information exchanged and also enhanced effectiveness of the responsible organization due to the exchange of information); and

– data and system security (confidentiality, integrity, availability, etc.)

IEC 80001-1 process

• Responsible organization establishes the process

• Based on ISO 14971

• Addresses hazards associated with the connection of medical devices to a network

• Residual risk is approved by appropriate person in the responsible organization
IEC 80001-1 Status

- Joint working group between IEC 62A and ISO 215
  - Todd Cooper and Sherman Eagles co-conveners
- First meeting held in January 2007
- Involvement by
  - Medical Device Manufacturers
  - Hospitals
  - FDA
- First committee draft circulated in December, 2007
- Second Committee draft circulated November, 2008
- Draft for vote will be circulated July 31
- Schedule for approved standard, end of 2010

Future standards activities

- Guidance documents to aid in implementation of IEC 80001-1
  - Guidance for Healthcare Delivery Organizations
  - Guidance for wireless networks
  - Guidance for the communication of medical device security needs, risks and controls
  - Guidance for development of responsibility agreements
  - Step-by-step risk management with examples
  - Causes of hazards associated with medical IT-networks
Another future activity?

- Guidance for writing documentation and code for effective implementation of static analysis

Sherman Eagles
seagles@softwarecpr.com
612-865-0107

Offering training and consulting on medical device software validation and software risk management

www.softwarecpr.com