

# New IEC Guidance on the Application of ISO 14971 to Medical Device Software

By David Walker

Most medical device R&D organizations engineering software intensive devices are currently piecing together ISO 14971 “Medical devices — Application of risk management to medical devices” and AAMI (Association for the Advancement of Medical Instrumentation) TIR 32 “Medical device software risk management” to ensure an effective and FDA compliant safety risk management strategy for software.

The AAMI Medical Device Software Committee recently reviewed a committee draft of a new IEC TR 80002 (Medical device software – Guidance on the application of ISO 14971 to medical device software) that provides guidance on the application of ISO 14971 to medical device software. This report is effectively a globalization of the AAMI TIR 32 that established consensus in the US on software risk management philosophy and strategy for medical devices. This short article will summarize the contents and key points of this new guidance that is expected to reach global consensus in 2009:

Details:

## **IEC TR 80002**

**Title:** Medical device software – Guidance on the application of ISO 14971 to medical device software

**Ballot Committee:** IEC/SC 62A, Common Aspects of Electrical Equipment Used in Medical Practice

**Committee Author:** IEC/SC 62A/JWG 03, Joint IEC/SC 62A-ISO/TC 210 WG: Medical device software (ISO/TC 210/JWG 02)

**Tag:** AAMI/SW, Medical Device Software Committee

The Committee Draft (CD) was prepared by the IEC Sub Committee 62A Joint Working Group (JWG) 3 between IEC Sub Committee 62A and ISO Technical Committee 210.

Firstly, the document structure of IEC 80002 matches that of ISO 14971. This makes it very easy for those familiar with ISO 14971 to find things. Even the section numbers and subsection titles match. An overall perspective would be that this technical report clarifies the application to software for each section of ISO 14971. One might also say the this technical report takes the information provided in AAMI TIR 32 and folds it into the outline of ISO 14971. The draft is currently 66 pages long and contains much detail with regard to software aspects of safety risk management.

In section 3, General requirements for risk management, warns against segregation of software risk management from overall system or device risk management. Often, there are opportunities to mitigate system safety risks with software safety features, and to mitigate software risks with system

safety features. The involvement of software engineering personnel in hazard analysis and overall risk management process is critical to software intensive medical device safety.

Other points within this section include the iterative nature of software risk management, the difficulty in estimating software risk probability, proactive safety management, and some great detail in software engineering aspects of safety.

In section 4, Risk analysis, various methods are discussed for risk assessment such as Fault Tree Analysis (FTA, see IEC 61025), Failure Mode Effects Analysis (FMEA, see IEC 60812), and Hazard and Operability Study (HAZOP, see IEC 61882) and the value of such approaches in various situations. It is stressed that due to the difficulty in estimating probability for software failure, the probability should be set to 1, and the rigor in mitigating the risk should be commensurate with the severity of the hazard.

Some work has started at the SEI (Software Engineering Institute) to establish structure for “Goal Structured Assurance Cases” as a method of software assurance. A goal-structured assurance case specifies a claim regarding a property of interest, evidence that supports that claim, and a detailed argument explaining how the evidence supports the claim. This is ground breaking work to provide a replacement for reliability studies in building confidence in software safety. Follow this link to section 5 of the report: <http://www.sei.cmu.edu/pub/documents/08.reports/08tr025.pdf>

In section 5, Risk Evaluation, early consideration of risk exposure is stressed to provide adequate mitigation. Hazards are traced to software components so that action can be taken to mitigate the risk of software components contributing to hazards.

In section 6, Risk control, the concept of last point of control, is discussed. Where a hazardous condition could result in a chain of events, it is often effective to consider risk control measures for the last event. This increases the chances of trapping loosely coupled causes which have unpredictable effects and may have been missed in risk analysis.

Risk management considerations for Software Of Unknown Provenance (SOUP) is also covered.

Section 7, Evaluation of overall residual risk acceptability, and 8, Risk management report, do not have much elaboration for software.

In section 9, Production and post-production information, the maintenance cycle is discussed. Considerations are made for updates to developed software or SOUP and risks associated with these changes.

There are four annexes:

Annex A (informative) Discussion of Definitions

Annex B (informative) Direct causes example

Annex C (Informative) LOOSELY COUPLED CAUSE/RISK CONTROL MEASURE

*An excellent source for developing coding and design standards*

Annex D (Informative) POTENTIAL PITFALLS

Annex E (Informative) Life cycle/RISK MANAGEMENT grid

The ASQ Software Division newsletter will announce when the new IEC 80002 technical report is released and available for purchase. Watch for the spring edition of this newsletter in which a summary will be provided for another important IEC standard currently undergoing domestic review by the AAMI Medical Device Software Standards Committee, **IEC 80001 Application of risk management for IT-networks incorporating medical devices.**

*David Walker is the immediate past chair of the ASQ Software Division. He represents ASQ's interests in medical device software standards development through membership on the AAMI Medical Device Software Standards Committee.*