SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

Standards Navigator

Standards Navigator Monthly Report

7-July-2015

SoftwareCPR Standards Navigator provides information and tools related to standards that play a significant role in health software and software intensive medical devices. In addition to information on existing standards, SoftwareCPR Standards Navigator keeps you up to date on new standards activity and gives you expert insight into future changes to existing standards.

http://www.softwarecpr.com/topicsframepage.htm

June 2015 Standards Navigator Overview

Medical device software

- The IEC 62304 amendment has been published as edition 1.1, a consolidated redline version. IEC 62304 Edition 1.1 is available from IEC. AAMI will publish an ANSI/AAMI version in the future. Edition 1.1 is expected to replace edition 1 as an EU harmonized standard, but there is no timetable for this at present.
- A draft for ballot of *IEC 82304-1 Health Software: General requirements for safety* was sent to IEC in early May. The draft is currently being translated into French before being circulated for review and voting. The draft is expected to be circulated as a committee draft with vote (CDV) in July. This standard will be voted on concurrently by CENELEC and is expected to become a harmonized EN document. Conformance to this standard is expected to provide assumption of conformity to the software validation portion of the MDD essential requirement on software for those products that are only software.
- The working group developing the second edition of IEC 62304 is meeting in September. Their schedule calls for a first committee draft to be available for review by the end of October.
- A committee draft of a new technical report, *IEC 80002-2: Medical device software – Part 2: Validation of software for regulated processes* has been circulated for comment. This technical report applies to any software used to automate device design, testing, component acceptance, manufacturing, labeling, packaging, distribution, and complaint handling or to automate any other aspect of a medical device quality system, as defined by ISO 13485. It applies to
  – Software used in the production of a device, and
  – Software used in implementation of the device manufacturer's quality system.
  It does not apply to:
  - software used as a component, part, or accessory of a medical device, or
  - software that is itself a medical device.
  This TR is expected to be used as guidance by auditors of 13485 to assess the compliance to new requirements for software validation in the revision of 13485 currently in progress.

  The draft Technical Report is available on the SoftwareCPR Standards Navigator web page.

Medical Devices

- A draft of *IEC TR 62366-2: Medical devices – Part 2: Guidance on the application of usability engineering to medical devices* has been circulated for vote. This technical report provides medical device manufacturers with guidance on how to integrate usability engineering (also called human factors engineering) principles and user interface design practices into their overall medical device development processes. An appropriate-tailored investment in usability engineering ensures that medical devices will have acceptable risk and usability and that design shortcomings are identified and removed from the user interface. Accordingly, this technical report emphasizes the importance of designing for usability, with an emphasis placed on ensuring safety. This technical report is not intended to be used for regulatory purposes. It contains no requirements and only provides guidance.

  The draft is available on the SoftwareCPR Standards Navigator web page.

Health IT and mobile health applications

- No new documents this month.

Security

- The National Electrical Manufacturers Association (NEMA) has published a guidance document on supply chain best practices for electrical equipment and medical imaging manufacturers to minimize the possibility that bugs, malware, viruses, or other exploits can be used to negatively impact product operation. The document is a representation of identified best practices that vendors can implement as they develop, manufacture, and deliver products as part of the supply chain. The document addresses supply chain integrity through four phases of the product life cycle: manufacturing and assembly, tamper-proofing, security development life cycle, and decommissioning/revocation.

  The NEMA guidance document is available at http://www.nema.org/Standards/Pages/Supply-Chain-Best-Practices.aspx.

- A draft for vote (DTR) of *IEC TR 80001-2-8: Application of risk management for IT networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2* has been circulated.
  This part of IEC 80001 provides guidance for the application of the framework outlined in IEC 80001-2-2. Managing the risk in connecting medical devices to IT-networks requires the disclosure of security-related capabilities and risks. IEC 80001-2-2 presents a framework for this disclosure and the security dialog that surrounds the IEC 80001-1 risk management of IT-networks. IEC 80001-2-2 presents an informative set of common, descriptive, security-related capabilities that are useful in terms of gaining an understanding of user needs. IEC 80001-2-8 addresses each of the security capabilities and identifies security controls from six standards for consideration by all stakeholders during risk management activities, supplier selection, device selection etc.
  The six standards that the controls are from are:
  – NIST SP 800-53, Revision 4, Recommended Security Controls for Federal Information Systems and Organizations
  – ISO/IEC 15408-2:2008, Information technology – Security techniques – Evaluation criteria for IT security -- Part 2: Security functional components
  – ISO/IEC 15408-3:2008, Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components
  – ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls
  – ISO 27799:201x, Health informatics – Information security management in health using ISO/IEC 27002
  – IEC 62443-3-3:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

  The draft is available on the SoftwareCPR Standards Navigator web page

Software Engineering and Information Technology

- A final draft for vote (FDIS) of *ISO/IEC/IEEE 24748-4 Systems and software engineering — Life cycle management — Part 4: Systems engineering planning* has been circulated.

  This International Standard:
  - specifies the Technical management processes from ISO/IEC/IEEE 15288 that are required to be implemented for planning a systems engineering project,
  - gives guidelines for applying the required processes,
  - specifies a required information item, a plan for the technical management and execution of the project, that is to be produced through the implementation of the Project Planning process,
  - gives guidelines for the format and content of the required information item, and
  - provides normative definition of the content of the information item, that results from the application of these processes to that end. In this International Standard that plan for technical project management is termed the Systems Engineering Management Plan (SEMP).

The draft is available on the SoftwareCPR Standards Navigator web page

- A third committee draft (CD) of *ISO/IEC 24748-5 Systems and software engineering — Life cycle management — Part 5: Software development planning* has been circulated.

  This international standard provides a common framework for planning and controlling the technical processes and activities to produce and sustain software products. The complete life cycle is covered by this standard, from idea conception to the retirement of a software product. The framework described by this standard provides for best practices in communication and cooperation among parties that plan for, develop, utilize, and manage modern software.

  This international standard
  - specifies the required information items to be produced through the implementation of the required planning and control processes,
  - specifies the required content of the required information items, and
  - gives guidelines for the format and content of the required and related information items.

  The draft is available on the SoftwareCPR Standards Navigator web page

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents can be found on the SoftwareCPR Standards Navigator until their review period completes.

	Topic	Use / Users	Description
ISO/IEC Guide 63 Draft	Risk management	Manufacturers	ISO/IEC Guide 63 - Guide to the development and inclusion of aspects of safety in International Standards for medical devices
ISO/IEC 29119-5 DIS	Software engineering	Manufacturers	ISO/IEC 29119-5 - Systems and software engineering. Keyword driven testing. Draft for vote.
ISO/IEC/IEEE 12207 DIS	Software Engineering	Manufacturers	*ISO/IEC 12207 - Systems and software engineering — Software life cycle processes* Draft for vote. This new revision of ISO/IEC/IEEE 12207 is the product of a coordinated effort by IEEE and ISO/IEC JTC 1/SC 7 to completely harmonize life cycle process standards for systems and for software.

REFERENCE LIBRARY

	Topic	Use / Users	Description
ONC 10-Year Vision	Health IT	Health IT infrastructure	*ONC 10-Year Vision to Achieve an Interoperable Health IT Infrastructure* The document can be found on the SoftwareCPR Standards Navigator web page or at http://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf
BSI white paper	Medical devices	Manufacturers	*"The proposed EU regulations for medical and in vitro diagnostic devices"* The white paper can be found on the SoftwareCPR Standards Navigator web page
EC green paper	Health IT	Manufacturers	*"Green Paper on mobile Health (mHealth)"* The green paper can be found on the SoftwareCPR Standards Navigator web page
IMDRF SaMD Definitions	Software	Manufacturers	Software as a Medical Device (SaMD): Key Definitions Report on international harmonization of definitions for software as a medical device. Adopted by IMDRF in November 2013. ***The report can be found on the SoftwareCPR Standards Navigator web page.***

Euro Commission	Medical Devices	Manufacturers	Commission recommendation of 24 September 2013 on the audits and assessments performed by notified bodies in the field of medical devices. ***The document can be found on the SoftwareCPR Standards Navigator web page.***
FDA Safety communication on cybersecurity	Security	Manufacturers and hospitals	FDA has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations. This safety communication recommends that medical device manufacturers take steps to limit opportunities for unauthorized access to medical devices and hospitals take steps to evaluate network security and protect the hospital systems. The FDA also recommends prompt reporting of events that have impacted the performance of a medical device or hospital network.
ICS-CERT Alert regarding medical devices with hard-coded passwords	Security	Manufacturers, hospitals	ICS-CERT is issuing this alert to provide early notice of a report of a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. According to their report, the vulnerability could be exploited to potentially change critical settings and/or modify device firmware. The alert also identifies baseline mitigations for reducing risks to these and other cybersecurity attacks.
ONC Patient Safety Action & Surveillance Plan	Health IT safety	Health IT manufacturers, hospitals	The final version of the ONC plan that has the objectives to use health IT to make care safer and to continuously improve the safety of health IT.
ONC contract with the Joint Commission to investigate health IT-related safety events	Health IT safety	Hospitals, health IT manufacturers	The purpose of this contract is to ensure that there is an early detection system on health IT-related safety issues, including those associated with EHRs.

ONC guidance on annual surveillance plans by authorized certification bodies	Surveillance of certified EHRs	Authorized EHR certification bodies	Authorized Certification Bodies are expected to conduct surveillance on EHRs that they have certified. This guidance provides the priorities for topics to assess in the surveillance plan. Safety-related capabilities and security capabilities are two of the four areas for priority identified in this guidance.
TEAM-NB position paper on use of ISO 14971:2012	Risk management	Manufacturers	Describes the steps TEAM-NB members plan to verify where relevant if requirements of EN ISO 14971:2012 have been met. This should help manufacturers update their risk management procedures and files to maintain compliance with the Essential Requirements of the directives, when building on the presumption of conformity. ***The position paper can be found on the SoftwareCPR Standards Navigator web page.***
TEAM-NB "Vision on Revision"	Regulation	Regulators, Manufacturers, Notified bodies	This document forms the input of TEAM-NB into the debate on The Revision of European Legislation on Medical Devices. Contributions came from BSI Germany, BSI UK, DEKRA Netherlands, TUV Austria, and TUV Sud. ***The report can be found on the SoftwareCPR Standards Navigator web page.***
Report	Interoperability	Medical device manufacturers, Hospitals, Regulators	AAMI/FDA Interoperability Summit report An AAMI/FDA sponsored summit meeting on medical device interoperability was held in late 2012. This report documents the discussion and identifies themes from the summit. This report can be found at http://www.aami.org/interoperability/Interoperability_Summit_publication.pdf

Report	Wireless	Hospitals, Medical device manufacturers	AAMI Wireless Workshop report A workshop with approximately 80 invited medical wireless experts was held in late 2012. This report documents the discussion and outcomes of this workshop. A follow-up meeting is planned for March 2013. This report can be found at http://www.aami.org/wireless/2012_Wireless_Workshop_publication.pdf

Report	Security	Medical device manufacturers, Regulators	GAO report on FDA review of certain medical devices The General Accounting Office does investigations for the US Congress. In this report they reviewed how FDA reviewed implanted medical devices that used wireless communications for security vulnerabilities that could cause safety concerns. They looked at two devices that researchers had shown could be controlled by use of off-the-shelf radio devices. In their findings, they criticized FDA for not reviewing security capabilities in these devices, even though they determined that FDA had the authority to do so. This will certainly result in FDA increasing their scrutiny of security for these type of devices. Since a security vulnerability in a device that is wirelessly communicating over a network seems to surely pose a risk as well, it is likely that FDA will also increase security scrutiny of all devices that use wireless communications. Dr. Kevin Fu testified to the National Institute of Standards and Technology Information Security & Privacy Advisory Board that "Conventional malware is rampant in hospitals because of medical devices using unpatched operating systems. There's little recourse for hospitals when a manufacturer refuses to allow OS updates or security patches." A report of the meeting can be found in the MIT Technology Review http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/ The article states that “In September, the Government Accountability Office issued a report warning that computerized medical devices could be vulnerable to hacking, posing a safety threat, and asked the FDA to address the issue. The GAO report focused mostly on the threat to two kinds of wireless implanted devices: implanted defibrillators and insulin pumps. The vulnerability of these devices has received widespread press attention (see "Personal Security" and "Keeping Pacemakers Safe from Hackers"), but no actual attacks on them have been reported. Fu, who is a leader in researching the risks described in the GAO report, said those two classes of device are "a drop in the bucket": thousands of other network-connected devices used for patient care are also vulnerable to infection. "These are life-saving devices. Patients are overwhelmingly safer with them than without them. But cracks are showing," he said. (Fu was *Technology Review's* Innovator of the Year in 2009.)” One of Dr. Fu’s collaborators in research that showed an implanted defibrillator could be hacked was Dr. William Maisel who is now the Deputy Director for Science at CDRH. FDA staff has indicated that they are in the process of revising the FDA Cybersecurity Guidance. This guidance will likely include recommendations for manufacturer’s security programs for devices and additional recommendations for security information to be provided during pre-market review of devices that are intended for use on a network. In addition, the guidance is now expected to provide information on when a security issue is reportable to the FDA and when a security event will result in a recall. Another interesting bit of information in this report was the FDA response that they had hired a consultant (later determined to be McKinsey) to assess how they review software and make suggestions for improvements. This assessment is supposed to be completed by the end of 2012.

Report	Mobile medical devices	Medical devices manufacturers, Hospitals, Regulators	FCC report on Mobile Medical Devices The FCC created an independent mHealth Task Force, to research the barriers to rapid deployment of mHealth technology and develop recommendations to government and industry to address those barriers. This report documents the task force recommendations for achieving 5 goals: Goal 1: FCC should continue to play a leadership role in advancing mobile health adoption. Goal 2: Federal agencies should increase collaboration to promote innovation, protect patient safety, and avoid regulatory duplication. Goal 3: The FCC should build on existing programs and link programs where possible in order to expand broadband access for healthcare. Goal 4: The FCC should continue efforts to increase capacity, reliability, interoperability and RF safety of mHealth technologies. Goal 5: Industry should support continued investment, innovation, and job creation in the growing mobile health sector. Recommendations include: • greater collaboration with other US Federal agencies • promoting the availability of broadband for healthcare • harmonizing spectrum allocations for healthcare internationally • industry use of standards based technologies for transmitting authenticated messages and encrypted health information ***This report can be found on the Standards Navigator web page***
Report	Health IT	Hospitals, EHR vendors, MD manufacturers	Institute of Medicine report – Health IT and patient safety The Institute of Medicine produced a report on the impact of Health IT on patient safety. The report had a number of recommendations for the Secretary of HHS. ***A presentation on the recommendations and the entire report are available at the SoftwareCPR Standards Navigator web page.***

Regulation	Regulation	Medical device manufacturers, IVD manufacturers	EU draft proposed new Medical Device Regulation and In-Vitro Device Regulation These draft regulations can be found at http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_542_en.pdf - medical devices http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_541_en.pdf - In-vitro devices

STANDARDS CURRENTLY UNDER DEVELOPMENT OR REVISION

	Topic	Use / Users	Description
IEC 62304 Edition 2	Software Life Cycle	Health Software Vendors including medical device manufacturers	The second edition expands the scope of 62304 from medical device software to health software. Health software is any software that is developed with an intended purpose of being used for health services. This includes software developed for medical devices. Current status: An initial committee draft is being developed. Next step: A draft is expected to be circulated in October 2015. Expected completion: 2018
IEC 82304-1	Health Software	Medical device manufacturers, Regulators	New standard on Health Software: General Requirements. This standard is intended to be for standalone software products and to cover the product level requirements such as product validation, labeling, documents to be provided to the user, etc. Current status: CDV has been registered with IEC. Next step: A CDV is expected to be circulated in fall 2015. Expected completion: 2016

ISO 13485	Medical devices	Medical device manufacturers, Regulators	The Quality Management System standard is being revised to bring it into alignment with ISO 9001:2008. Current status: Second DIS was approved in ISO but not in CEN. Next step: Resolve issues with CEN. Expected completion: 2016