Standards Navigator

Standards Navigator Monthly Report

1-November-2014

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

October 2014 Standards Navigator Overview

Medical device software

The IMDRF Management Committee approved the final N12 document, “Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations,” of the SaMD WG.

The approved final N12 document is available on the SoftwareCPR Standards Navigator web page and is posted on the IMDRF web site at http://www.imdrf.org/documents/documents.asp.

A Work Item Extension was also approved for the SaMD working group. “Applicability of Existing Quality Management System Requirements as a Risk Control Measure.” The WG is continuing the development of risk control measures under the Work Item Extension.

The Work Item Extension is available on the SoftwareCPR Standards Navigator web page.

Medical Devices

- A committee draft of ***IEC TR 60601-4-2: Medical electrical equipment - Part 4-2: Guidance and interpretation - Electromagnetic immunity; performance of medical electrical equipment and medical electrical systems*** has been circulated for comment. This International Technical Report provides guidance on achieving immunity with regard to electromagnetic compatibility (EMC) or EMC performance. Based on the intended use, medical electric equipment and medical electric systems should have adequate immunity to provide the performance specified by the manufacturer in the presence of electromagnetic disturbances.

Guidance for EMC is necessary because for some me equipment and me systems, the basic safety and essential performance might not include the purpose(s) for which the equipment or system was purchased. It is important to the operator or responsible organization and to the delivery of healthcare that these functions operate as intended in the EM environments of intended use.

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

- A Draft Technical Report of ***IEC TR 60878: Graphical symbols for electrical equipment in medical practice*** has been circulated for vote. This technical report is a comprehensive collection of all graphical symbols used on medical electrical equipment. It is intended for the easy finding of a certain symbol and related ones in one single source, concentrating on this special field of application.

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

Health IT and mobile health applications

No new documents. The IMDRF SaMD classification includes mobile and health IT applications that meet the definition of a medical device.

Quality

- The IMDRF has approved a Work Item Extension for the SaMD Working Group, “Applicability of Existing Quality Management System Requirements as a Risk Control Measure.” *The work item description is available on the SoftwareCPR Standards Navigator web page*.

Security

- No new documents. The FDA held a two day public workshop on Collaborative Approaches for Medical Device and Healthcare Cybersecurity on October 21-22. Documentation on the workshop including the video recording of the workshop can be found here under Webcast near the bottom of the page. http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm412979.htm
- The FDA held a webinar on their premarket cybersecurity guidance on October 29. In it they noted that the Instructions for Use should include what cybersecurity controls are needed in the use environment, but stated that it is not sufficient for a device to rely on a network being secure. The device manufacturer should identify the cybersecurity functions they have included in their device. Some of the core functions include:
  - Limiting access to trusted users by using layered privileges, appropriate authenticity, and strong passwords.
  - Protecting users and data by terminating sessions after a period of inactivity, setting up physical locks, and limiting access ports.
  - Detecting, responding and recovering by implementing features that tell a user if the device has been compromised, provide information on what to do when it occurs, implement features to preserve critical functions with the ability to reboot and recognize drivers, and provide methods for retention and recovery of device configuration.

  They also expect to see a hazard analysis program that clearly evaluates risk potential, provides information on control put in place and the appropriateness of those controls to mitigate an identified risk, and a matrix that links cybersecurity controls to the risk being mitigated. Since the threat landscape will be continually evolving, they also want to see a plan for how the manufacturer will manage evolving threats. In response to a question, they indicated that updates for cybersecurity needed to manage new threats do not require a new premarket submission. Other questions brought out these points:

  - Cybersecurity information is required for all submissions after October 1, 2014
  - Risk to the system as a whole must be acceptable
  - Mobile apps intended to control a device would need to consider cybersecurity
  - Cybersecurity should be considered for any programmable logic – that is hardware functionality that can be re-programmed
  - There is no requirement for minimum strength of encryption, but they expect a rationale from the manufacturer for the encryption chosen
  - A software device delivered from the cloud should consider environment and analyze it for cybersecurity risks
  - Labeling could be used to mitigate cybersecurity risks if it clearly informs the user of the needed mitigations

Software Engineering

- A committee draft (DIS) of ***ISO/IEC 15026-3 Systems and software engineering — Systems and software assurance — Part 3: Systems integrity levels*** has been circulated for vote. This International Standard specifies the concept of integrity levels with corresponding integrity level requirements that are required to be met in order to show the achievement of the integrity level. It places requirements on and recommends methods for defining and using integrity levels and their integrity level requirements. It covers systems, software products, and their elements, as well as relevant external dependences.
  The draft standard is available on the SoftwareCPR Standards Navigator web page.
- A committee draft (DIS) of ***ISO/IEC 25066 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Common industry Format for Usability — Evaluation Reports*** has been circulated for vote. This International Standard describes the Common Industry

Format (CIF) for reporting usability evaluations. It provides a classification of evaluation approaches and the specifications for the content items in an evaluation reports (content elements). The intended users of the usability evaluation reports are identified, as well as the situations in which the usability evaluation report can be applied.

The usability evaluation reports in this International Standard are applicable to software and hardware systems, products or services used for predefined tasks (excluding generic products, such as a display screen or keyboard). The content elements are intended to be used as part of system-level documentation resulting from development processes such as those in ISO 9241-210 and ISO/IEC JTC 1/SC 7 process standards. The content elements for documenting evaluations can be integrated in any type of process model.

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

- A committee draft (DIS) of ***ISO/IEC 19770-2 Information technology — Software asset management — Part 2: Software identification tag*** has been circulated for vote. This part of ISO/IEC 19770 provides an International Standard for software identification (SWID) tags. The software identification tag is a standardized data structure containing identification information about a software product that supports new and automated management functions.

  This part of ISO/IEC 19770 has been developed to facilitate automation of IT processes through the use of software identification tags and for applications which use tags, for the purposes of security, compliance and logistics automation.

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

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

ISO 27799 DIS	Security	Manufacturers	*ISO 27799 Health informatics — Information security management in health using ISO/IEC 27002* ISO 27799 applies ISO/IEC 27002 to the healthcare domain in a way that carefully considers the appropriate application of security controls for the purposes of protecting personal health information. The DIS can be found on the SoftwareCPR Standards Navigator web page.
ISO/IEC 15288 FDIS	System Engineering	Manufacturers	*ISO/IEC 15288 Systems and software engineering — System life cycle processes* This International Standard establishes a common process framework for describing the full life cycle of man-made systems from conception through retirement. This new version will replace the 2008 edition. The FDIS can be found on the SoftwareCPR Standards Navigator web page.
ISO/IEC 12207 CD	Software Engineering	Manufacturers	*ISO/IEC 12207 Systems and software engineering — Software life cycle processes* This International Standard establishes a common process framework for describing the full life cycle of software products (including software elements of systems) from conception through retirement. The CD can be found on the SoftwareCPR Standards Navigator web page.

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

ISO/IEC 24748-5 FDIS	Software Engineering	Manufacturers	*ISO/IEC 24748-5 Systems and software engineering — Life cycle management — Part 5: Software development planning* This International Standard unifies technical and management requirements and guidance from several sources to specify the requirements for the content of technical management and development plans, and provides common document formats. The FDIS can be found on the SoftwareCPR Standards Navigator web page.
ISO 9000 DIS	Quality	Manufacturers	*ISO 9000 - Quality management systems — Fundamentals and vocabulary.* The draft standard can be found on the SoftwareCPR Standards Navigator web page.
ISO 9001 DIS	Quality	Manufacturers	*ISO 9001 - Quality management systems — Requirements.* The draft standard can be found on the SoftwareCPR Standards Navigator web page.
ISO 25011 CD	Quality	Manufacturers	*Information technology – Service Quality Requirement and Evaluation (SQuaRE) – Service Quality Model* The draft standard can be found on the SoftwareCPR Standards Navigator web page.
ISO 29119-5 DIS	Software	Manufacturers	*Software and Systems Engineering — Software Testing — Part 5: Keyword-Driven Testing* The draft standard can be found on the SoftwareCPR Standards Navigator web page.

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

ISO 25022 CD	Quality	Manufacturers	*Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of quality in use* The draft standard can be found on the SoftwareCPR Standards Navigator web page.
FDA draft guidance for MDDS	Medical devices	Manufacturers	*Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices – Draft Guidance for Industry and Food and Drug Administration Staff* In this draft guidance FDA notifies MDDS manufacturers that it does not intend to enforce compliance with regulatory controls for this type of medical device. The draft FDA guidance is available at http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm401785.htm

REFERENCES

	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. ***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 Amendment 1	Software Life Cycle	Medical Device manufacturers, Regulators	Amendment to the Medical Device Software Life Cycle standard. This standard is harmonized in the EU. The amendment addresses software safety classification and how to be compliant with legacy software. Current status: Comments received on the CDV are being resolved. Expected completion: 2015
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: Comments received on the second CD are being resolved. Next step: A CDV is expected to be circulated in early 2015. Expected completion: 2015
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. Next step: Second DIS. Expected completion: 2016