SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

Standards Navigator

Standards Navigator Monthly Report

10-June-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

May 2014 Standards Navigator Overview

Medical device software

Medical Devices

- A draft of *IEC TR 62354: General testing procedures for medical electrical equipment* has been circulated for vote. This edition will replace and cancel the second edition which was published in 2009. This is a technical revision to align the guidance with Amendment 1 to IEC 60601:2005. Approximately 30 tests have been significantly revised.

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

- AAMI has circulated a draft of *AAMI TIR38 Medical device safety assurance case guidance* for comment. This draft is significantly revised from previous drafts with the addition of material developed by the FDA ODE reviewers who have been reviewing safety assurance cases. An assurance case is a systematic, structured methodology for supporting a stated claim. The claim may be related to safety, reliability, maintainability, security, etc. A safety assurance case is an assurance case with a top level claim of safety. The Medical Device Safety Assurance Case outlined in this technical information report (TIR) provides a comprehensive and organized summary of product risk along with the evidence-based arguments that support the claims that the hazards that may arise from risk has either been eliminated or mitigated to the extent that the product is safe for its intended use.

  The draft TIR is available on the Software Standards Navigator web page.

Health IT and mobile health regulation

- ONC has published a 10 year roadmap to achieving a “learning health system” that will result from an interoperable health IT ecosystem that makes the right data available to the right people at the right time across products and organizations in a way that can be relied upon and meaningfully used by recipients. By 2024, ONC believes that individuals, care providers, communities, and researchers should have an array of interoperable health IT products and services that allow the health care system to continuously learn and advance the goal of improved healthcare.

  The ONC 10-Year Vision to Achieve an Interoperable Health IT Infrastructure can be downloaded at
  http://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf

- A group established by ISO TC 215 to look at a standards framework for health software safety issued an interim report. The report proposes a framework of foundational standards that apply across the entire life cycle and three life cycle phases; development, implementation and clinical use. A final report will be completed by October, 2014.

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

Security

- A working draft of a second edition of *ISO 27799 Health informatics — Information management in health using ISO/IEC 27002* is being reviewed prior to circulating a draft for ballot. This international standard provides guidance to healthcare organizations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of such information. It is based upon—and extends—the general guidance provided by *ISO/IEC 27002 Information technology — Security techniques —Code of practice for information security controls* and addresses the special information security management needs of the health sector and its unique operating environments. It is not intended to supplant the ISO/IEC 27000 series of standards. Rather, it is a complement to these more generic standards. This guideline is consistent with the revised version of ISO/IEC 27002:2013.

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

- A new draft 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 for comment. This report presents the 19 SECURITY CAPABILITIES of IEC 80001-2-2, their respective “requirement goal” and “user need” (identical to that in IEC 80001-2-2) with a corresponding list of SECURITY CONTROLS from a number of security standards. The security standards that the controls were drawn from include: NIST SP 800-53, Revision 4, ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008, ISO/IEC 27002:2013, ISO 27799:2008, IEC 62443-3-3:2013.

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

- NIST has issued an initial public draft of *Special Publication 800-160 Systems Security Engineering.* This publication addresses the engineering-driven actions necessary for developing a more defensible and survivable information technology (IT) infrastructure—including the component products, systems, and services that compose the infrastructure. It starts with and builds upon a set of well-established International Standards for systems and software engineering published by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronic Engineers (IEEE) and infuses systems security engineering techniques, methods, and practices into those systems and software engineering processes.

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

Software Engineering

Activity – May 2014

NEW STANDARDS, REPORTS & REGULATIONS

	Topic	Use / Users	Description
IEC TR 62354 DTR	Medical devices	Manufacturers	*IEC TR 62354: General testing procedures for medical electrical equipment* The draft TR can be found on the SoftwareCPR Standards Navigator web page. The ballot closes on July 4.
AAMI TIR38	Medical Devices	Manufacturers	*AAMI TIR38 Medical device safety assurance case guidance* The draft TIR can be found on the SoftwareCPR Standards Navigator web page. The comments will be considered at a meeting on June 25.
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
ISO TC 215 standards framework for health software Safety	Health software	Manufacturers	*Health Software Ad hoc group Interim Report – May 2014* *Health Software Safety Standards* *FUTURE STATE Architecture/Framework – DISCUSSION DRAFT* The report can be found on the SoftwareCPR Standards Navigator web page.

NEW STANDARDS, REPORTS & REGULATIONS

	Topic	Use / Users	Description
ISO 27799 WD	Security	Manufacturers and hospitals	*ISO 27799 Health informatics — Information management in health using ISO/IEC 27002* The working draft can be found on the SoftwareCPR Standards Navigator web page.
IEC TR 80001-2-8 CD	Security	Manufacturers and hospitals	*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* The committee draft can be found on the SoftwareCPR Standards Navigator web page. Comment period closes on August 8.
NIST 800-160	Security	Manufacturers and hospitals	*NIST Special Publication 800-160 Systems Security Engineering* The initial public draft can be found on the SoftwareCPR Standards Navigator web page. The comment period ends July 11.

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

IEC 62304 Amd CDV	Medical device software	Manufacturers	*IEC 62304: Medical device software – Software life cycle processes* The CDV of the Amendment can be found on the SoftwareCPR Standards Navigator web page. The ballot closes on July 18.
ISO 16142-1 DIS	Medical devices	Manufacturers	*ISO 16142-1: Medical devices — Recognized essential principles of safety and performance of medical devices* The DIS can be found on the SoftwareCPR Standards Navigator web page
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
ISO 90003 FDIS	Software engineering	Manufacturers	*ISO 90003: Guidelines for the application of ISO 9001:2008 to computer software* The FDIS can be found on the SoftwareCPR Standards Navigator web page
ISO 15289, 2nd Ed FDIS	Software engineering	Manufacturers	*ISO 15289, 2nd Ed: Content of life-cycle information products (documentation)* The FDIS can be found on the SoftwareCPR Standards Navigator web page

ISO 24748-4 DIS	Software engineering	Manufacturers	*ISO 24748-4: Life cycle management — Part 4: Systems engineering planning* The DIS can be found on the SoftwareCPR Standards Navigator web page
ISO 24748-6 NP	Software engineering	Manufacturers	*ISO TS 24748-6: Life cycle processes — System integration engineering* The NP can be found on the SoftwareCPR Standards Navigator web page
FDASIA Health IT Report	Health IT	Manufacturers	*Proposed Strategy and Recommendations for a Risk-Based Framework* The draft proposal can be found on the SoftwareCPR Standards Navigator web page. The comment period ends July 7.
ISO/IEC/IEEE 12207 CD	Software engineering	Manufacturers	*ISO/IEC/IEEE 12207 Systems and software engineering — Software life cycle processes* The CD can be found on the SoftwareCPR Standards Navigator web page
ISO/IEC 15026-3 CD	Software engineering	Purchasers and Manufacturers	*ISO/IEC 15026-3 Systems and software engineering —Systems and software assurance — Part 3: Systems integrity levels* The CD can be found on the SoftwareCPR Standards Navigator web page
ISO/IEC 29119-5 CD	Software engineering	Manufacturers	*ISO/IEC 29119-5 Software and Systems Engineering — Software Testing — Part 5: Keyword-Driven Testing* The CD can be found on the SoftwareCPR Standards Navigator web page
ISO/IEC 25011 CD	Information Technology	Service procurers and providers	*ISO/IEC 25011 Information technology — Service Quality Requirement and Evaluation (SQuaRE) – Service Quality Model* The CD can be found on the SoftwareCPR Standards Navigator web page

ISO/IEC/IEEE 15288 DIS	System Engineering	Manufacturers	*ISO/IEC/IEEE DIS 15288:201x(E) 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. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page. Ballot ends June 27.***

REFERENCES

	Topic	Use / Users	Description
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 draft premarket cybersecurity guidance	Security	Manufacturers	Recommendations for security controls to assure medical device cybersecurity and documentation to submit in a premarket review to demonstrate effective cybersecurity management. Recommends identifying cybersecurity risks and providing a traceability matrix that links cybersecurity controls to cybersecurity risks that were identified. Also recommends documentation to demonstrate that the device will be provided to purchasers free of malware and a plan for providing updates and patches to provide up-to-date protection.
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.
NIST draft outline of a cybersecurity framework for critical	Security	Hospitals, manufacturers	NIST was directed to prepare a cybersecurity framework for critical infrastructure in Presidential Executive Order 13636. Healthcare was identified as one of the areas with critical infrastructure. This draft for comment is only an outline of the framework. NIST intends the framework to take a risk management approach at a high level, focusing on key functions of cybersecurity management which are broken down into categories and subcategories. References such as existing standards, guidelines and practices will be provided for each

infrastructure			subcategory. A draft of the framework will be released in October.
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

Presentation	Research	Medical device manufacturers	Medical Device Innovation Consortium (MDIC) Presentation from FDA and MDIC FDA and Life Science Alley have been collaborating on establishing a public-private partnership for research into regulatory science. A non-profit organization called the Medical Device Innovation Consortium has been created. This presentation by the FDA and the temporary director of the non-profit describes the need and the plans for this organization. ***This presentation can be found on the Standards Navigator web page.***
Announcement	Interoperability	Medical device manufacturers, Hospitals, Regulators	AAMI/UL collaboration on interoperability standards AAMI and UL have announced that they will collaborate on a series of standards for medical device interoperability. The press release announces the collaboration and its benefits. This announcement can be found at http://www.aami.org/news/2012/091712_press_AAMI_UL_Interoperability.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. This report can be found at http://www.gao.gov/products/GAO-12-816

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 first CD are being resolved. Next step: Second CD or CDV will be circulated. Expected completion: January 2014
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: Second CD has been circulated. Ballot closing February 28, 2014. Next step: Comments on second CD will be resolved and a CDV circulated. Expected completion: 2015

IEC 62366-1	Medical devices	Medical device manufacturers, Regulators	The standard on human factors engineering is being revised and divided into two documents. The first is a standard that includes requirements for the process. The second will be a technical report providing information about good practices for implementing the human factors process. This document is the first part. Current status: Comments have been resolved on the first CD and a second CD circulated. Next step: Comments received on the second CD. 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. Current status: Comments have been received on the first CD and are being resolved. Next step: Second CD or DIS. Expected completion: 2015