SoftwareCPR®
Crisis Prevention And Recovery, LLC

Standards Navigator

Standards Navigator Monthly Report

8-July-2013

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 2013 Standards Navigator Overview

Medical device software

- IEC 62304 will have an amendment followed by a second edition that will expand the scope from medical device software to health software. A committee draft of the amendment has been circulated for review and comment. The major areas of change are to how the software safety class is determined and to requirements for legacy software. The draft proposes that the software safety class determination be based on risk, not just on severity. For legacy software that has been placed on the market before 62304 was in place, basic documentation must be in place and a gap analysis must be performed. If necessary, some additional documentation may need to be created.
- The EU movement toward a new medical device regulation slowed down this month when two parliament committees postponed meetings on the draft. However, work continues on parts of the draft, including definitions related to software. New implementing rules for the classification rules are being considered. These include removing the term "standalone software" because of concern that the definition may lead to confusion between software that is placed on the market separately from a device but subsequently integrated with the device and software that is a medical device in itself. This seems to be going in an opposite direction from the IMDRF which has a definition of "standalone software" in their draft definition document. The EU also proposed a term "software module" that means software that is associated with a specific application for the user which does not appear in the IMDRF draft definitions.
- The International Medical Device Regulators Forum work item on the international harmonization of the approach to standalone medical device software has been working on the definition of common data elements describing medical devices through the regulatory lifecycle. A draft is out for public review, with finalization planned for November. A draft description of how risk is determined for standalone medical device software is planned for November with final version in March, 2013. A draft of how to determine appropriate regulatory requirements is planned for March 2013 with a final version ready by September, 2013.

Health IT and mobile health regulation

1. The FDA Safety and Innovation Act (FDASIA) workgroup has continued meeting in three sub-groups to look at the specific areas of taxonomy, risk assessment and innovation, and regulations. The risk assessment and innovation sub-group is looking at both safety and risk to innovation. The workgroup plans to complete its input by the end of July and a draft report is expected by the end of September. The agencies have until January to complete the report.
2. The ONC released the final Patient Safety Action & Surveillance Plan. The objectives of the plan are to:

    1. Use health IT to make care safer
    2. Continuously improve the safety of health IT

    The plan has three strategies; learn, improve and lead. The strategies and related actions respond to the IOM report on Health-IT and Patient Safety published in 2012. They specifically call for improved reporting of adverse events and sharing of data, using meaningful use to establish and advance health IT patient safety priorities. In addition, ONC plans to incorporate safety into its standards and certification criteria by requiring safety principles to be included in software design and development, such as identifying the method used to incorporate user-centered design and providing transparency regarding their approach to "quality management systems" in the development of their products. ONC will encourage private sector leadership and shared responsibility for health IT patient safety. The plan states that it is different from the FDASIA report in that it lays out immediate and short-term actions while the FDASIA report will focus on responding to the requirement for a strategy and recommendations for a future regulatory framework.
3. ONC awarded a contract to The Joint Commission to investigate health-IT related deaths, serious injuries, or unsafe conditions. The intention is to provide ONC with an early detection system on health IT-related safety issues, including those associated with EHRs.
4. ONC also issued guidance on what surveillance is expected on EHRs and EHR Modules that have been certified. The Authorized Certification Bodies (ACB) surveillance plan should include how they will conduct surveillance initiated by complaints from a user and systematically obtain and synthesize feedback from users to determine if certain EHR capabilities should be evaluated to determine if they

continue to function as intended. Safety-related and security-related aspects are two of four criteria to be prioritized for surveillance plans.

5. ISO TR 17791 Health informatics Guidance on standards for enabling safety in health software has been approved with comments. A final draft with the comments resolved is being reviewed. It will be published later this year.

Usability

- ISO 62366 is being divided into two parts, Part 1 which is requirements and Part 2 which is recommended practices. A second committee draft of ISO 62366-1 has been circulated for review.

Security

- FDA released a draft guidance document on what should be submitted on cybersecurity for a premarket review.
- FDA also released a safety communication on cybersecurity for medical devices and hospital networks. The FDA is recommending that medical device manufacturers and health care facilities take steps to assure that appropriate safeguards are in place to reduce the risk of failure due to cyberattack, which could be initiated by the introduction of malware into the medical equipment or unauthorized access to configuration settings in medical devices and hospital networks. The FDA recommended steps that medical device manufacturers and hospitals should take to limit unauthorized access to medical devices and protect the hospital network.
- An alert was issued by the US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for medical devices hard-coded passwords. This security vulnerability exists in roughly 300 medical device across approximately 40 vendors. According to a Cylance report, the vulnerability could be exploited to potentially change critical settings and/or modify medical device firmware.
- NIST has released a draft outline of its cybersecurity framework for critical infrastructure. This framework was required to be developed by NIST by a Presidential Executive Order in February 2013. Healthcare is one of the critical infrastructures that will be covered by the framework. The draft outline shows what NIST expects the contents of the document to be and describes the sections. A draft of the framework will be made available in October.

Activity – June 2013

NEW STANDARDS, REPORTS & REGULATIONS

	Topic	Use / Users	Description
IEC 62304 Amendment 1 CD	Medical device software	Manufacturers	Revision of IEC 62304 has been divided into two parts, an amendment and a second edition. The amendment includes a revision to how software safety classification is determined and new requirements for legacy software that was developed prior to 62304, as well as a few other new requirements and clarification of existing requirements. A committee draft of the amendment has been circulated for comment. The second edition of 62304 will extend the scope to health software. Work on the second edition will begin later this year. ***The draft amendment can be found on the SoftwareCPR Standards Navigator web page.***
ISO 62366-1 CD2	Usability	Manufacturers	Requirements for usability. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
ISO 17522 DTR	Mobile Devices	Manufacturers	This technical report describes the status and requirements of health applications and services on smart devices platforms and suggests the reference architecture for these. ***The draft technical report can be found on the SoftwareCPR Standards Navigator web page.***

NEW STANDARDS, REPORTS & REGULATIONS

	Topic	Use / Users	Description
ISO 33001 DIS	Process assessment	Manufacturers	ISO IEC 33001 DIS Information technology — Process assessment — Concepts and terminology This International Standard provides a glossary of terms related to the performance of process assessment, together with an overall introduction to the concepts and standards framework for process assessment. The Standard identifies the principal components supporting the performance of process assessment, describes the results of process assessment, and gives an overview of the ways in which the results of assessment can be applied. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
ISO 33002 DIS	Process assessment	Manufacturers	ISO IEC 33002 DIS Information Technology — Process Assessment — Requirements for performing process assessment This International Standard defines the minimum set of requirements for performing an assessment that will ensure assessment results are objective, consistent, repeatable and representative of the assessed processes. The requirements help to ensure that the assessment output is self-consistent and to provide evidence to substantiate the ratings and to verify compliance with the requirements. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
ISO 33003 DIS	Process assessment	Manufacturers	ISO IEC 33003 DIS Information technology — Process assessment — Requirements for process measurement frameworks This International Standard provides requirements for process measurement frameworks that support and enable the assessment of process quality characteristics, from conceptualization to empirical validation. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***

NEW STANDARDS, REPORTS & REGULATIONS

	Topic	Use / Users	Description
ISO 33004 DIS	Process assessment	Manufacturers	ISO IEC 33004 DIS Information technology — Process assessment — Requirements for process reference, process assessment and maturity models This International Standard provides requirements for the construction and verification of process reference models, process assessment models and maturity models. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
ISO 33020 DIS	Process assessment	Manufacturers	ISO IEC 33020 DIS Information technology — Process assessment — Process measurement framework for assessment of process capability This International Standard defines a process measurement framework conformant to the requirements defined in ISO/IEC 33003 for the process quality characteristic of process capability. The process measurement framework in this international standard conforms to the requirements of ISO 33003 and is applicable to any domain. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
IMDRF draft document on Standalone Medical Device Software: Key Definitions	Medical device software	Manufacturers	The International Medical Device Regulators Forum believes that existing regulations do not readily address the unique public health risks posed by standalone software nor assure an appropriate balance between patient/consumer protection and promoting public health by facilitating innovation. The IMDRF has undertaken an effort to facilitate international regulatory convergence towards a smart, balanced regulatory approach that provides an optimal level of patient safety while fostering innovation and provides patient and providers with continued access to advanced health care technology that is safe. This draft document is the first of several documents intended to achieve these objectives. It identifies and defines key terms needed for regulation of standalone medical device software.

NEW STANDARDS, REPORTS & REGULATIONS

	Topic	Use / Users	Description
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. This is a draft for comment. Comments should be submitted before September 13.
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.

NEW STANDARDS, REPORTS & REGULATIONS

	Topic	Use / Users	Description
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 infrastructure	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 subcategory. A draft of the framework will be released in October.

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

ISO 13485 edition 3 – CD	Quality management systems	Manufacturers	This new edition of ISO 13485 is based off ISO 9001:2008. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***
IEC NP	Medical electrical equipment and medical electrical systems employing a degree of autonomy	Manufacturers	This Technical Report is intended to help a MANUFACTURER through the key decisions and steps required to perform a detailed RISK ASSESSMENT of MEDICAL ELECTRICAL EQUIPMENT or a MEDICAL ELECTRICAL SYSTEM, hereafter referred to as ME EQUIPMENT or ME SYSTEM, which employs a degree of autonomy. This Technical Report provides guidance on: • defining DEGREE OF AUTONOMY and by way of example give guidance on how this can affect the RISK ASSESSMENT; • methodologies for assessing the change to the RISK, and RISK reduction suggestion; and • BASIC SAFETY consideration in relation to IEC 60601-1. This is the first document created by a joint working group of IEC SC 62A – medical electrical equipment, and ISO/TC 184/SC 2 - Automation systems and integration - Robots and robotic devices. ***The draft technical report can be found on the SoftwareCPR Standards Navigator web page until September 6, 2013***

IEC 62657-2 Ed 1.0 - FDIS	Wireless communicatio n networks - Coexistence management	Hospitals, manufacturers	IEC 62657-2: Industrial communication networks - Wireless communication networks - Part 2: Coexistence management Wireless communication interfaces can interfere with others on the same premises or environment, disturbing each other. Therefore, without a predictable assuredness of coexistence, it could be problematic to have multiple wireless communication networks in the same facility or environment, especially because the time-criticality, the safety and the security of the operation may not be ensured in such an environment. This part of the IEC 62657 addresses the coexistence management for a predictable assuredness of coexistence. While this standard addresses industrial automation, the concerns are also applicable to healthcare delivery organizations. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page until July 19, 2013.***
ISO/IEC 29119-4 - DIS	Software testing – test techniques	manufacturers	ISO/IEC 29119-4 Software and Systems Engineering — Software Testing — Part 4: Test Techniques describes a set of techniques that have wide acceptance in the software testing industry. It is intended to be used during the test design and implementation process that is defined in ISO/IEC 29119-2 Test Processes. Risk-based testing can be used to determine the set of techniques that are applicable in specific situations. ***The draft standard can be found on the SoftwareCPR Standards Navigator web page.***

REFERENCES

	Topic	Use / Users	Description
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: Comments received on the first CD are being resolved. Major issues are scope and terminology. Next step: Second CD will be 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